Engineer

Courriel

courrier envoyé entre boîtes électroniques par Internet

Ce que c’est

Le courriel est le système qui transporte un message écrit vers une adresse de la forme `name@domain` et le laisse dans une boîte aux lettres jusqu’à ce que son destinataire le lise. En anglais, il s’écrit email ou e-mail ; les normes qui le définissent emploient généralement le simple mot mail. Rien n’exige que le lecteur soit en ligne au moment de l’envoi : des serveurs acceptent le message, le conservent et le transmettent. C’est pourquoi on parle de stockage et retransmission, plutôt que de conversation.

Deux documents définissent l’essentiel. La RFC 5322 décrit le message : un bloc de champs d’en-tête, une ligne vide, puis le corps. La RFC 5321 décrit SMTP, le protocole par lequel un serveur expéditeur remet ce message au serveur suivant sur son trajet. Pour trouver ce dernier, l’expéditeur consulte dans le DNS les enregistrements d’échange de courrier (MX) du domaine, qui désignent les machines acceptant le courrier destiné à ce domaine.

Un message complet peut être très court :

```
From: Ana Holm <ana@example.org>
To: orders@example.com
Date: Fri, 16 Oct 2026 09:14:00 +0200
Subject: Invoice 114 has the wrong VAT number
Message-ID: <20261016.0914.ana@example.org>

Hello, could you send a corrected copy?
```

Seuls deux de ces champs d’en-tête sont obligatoires : la date et l’adresse de l’auteur. Tout le reste est facultatif à la lettre de la norme, même si un message sans objet ou sans identifiant paraît négligé aux programmes qui trient le

courrier. Les lignes ne peuvent pas dépasser 998 caractères et devraient rester dans une limite de 78 : de nombreux logiciels de messagerie tronquent ou replient encore les lignes plus longues.

Il existe une seconde couche, cachée. SMTP transporte le message dans une *enveloppe* : une adresse de retour, où arrivent les rapports d'échec, et une liste de destinataires. L'enveloppe et les lignes `From:` et `To:` visibles par le lecteur sont distinctes et souvent différentes. Une copie cachée fonctionne parce que son destinataire figure dans l'enveloppe et pas dans les en-têtes. Une liste de diffusion fonctionne parce que l'adresse de retour de l'enveloppe pointe vers la liste : le rejet pour un abonné dont l'adresse n'existe plus arrive ainsi au logiciel de la liste, plutôt qu'à la personne qui a écrit le message.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce qu'un courriel ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Un site rapide, facile à trouver et modifiable par votre équipe, sans facture à chaque changement de texte.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 100 applications web avec HTML/HTML5 — 100 applications web développées

100 applications web avec HTML/HTML5 Contactez-nous →

Pourquoi c'est important

L'adresse électronique est l'identité sur laquelle repose une grande partie du web en dernier recours. Confirmations d'inscription, réinitialisations de mots de passe, reçus, factures et alertes de rejet d'un paiement passent tous par le courrier. Un produit dont les messages se perdent laisse donc des utilisateurs bloqués sans que personne s'en aperçoive. La personne qui n'a jamais reçu son lien de confirmation écrit rarement pour le signaler. Elle part.

Le courriel n'a pas non plus de propriétaire. Tout domaine peut exploiter ses propres serveurs et tout serveur peut communiquer avec un autre. Cette ouverture explique pourquoi il a survécu à presque tous les services de messagerie créés depuis. Le prix à payer est la confiance. La conception initiale laisse l'expéditeur écrire ce qu'il veut dans la ligne `From:` . Les serveurs destinataires décident donc eux-mêmes s'ils croient le message, à partir des preuves publiées par le domaine expéditeur dans le DNS : les hôtes autorisés à

envoyer pour lui, les clés qui signent ses messages et le traitement à réserver à un message qui revendique le domaine sans présenter ni l'une ni l'autre de ces garanties.

Pour une entreprise, la distinction utile sépare deux types de trafic. Le courriel transactionnel est adressé à une personne à la suite d'une action qu'elle vient d'effectuer : un code, un reçu, un lien de réinitialisation. Le courrier en nombre est adressé à de nombreuses personnes parce que l'expéditeur a choisi de l'envoyer. Ces trafics acquièrent des réputations distinctes, suscitent des plaintes à des fréquences différentes et partent souvent de domaines différents. Les mélanger permet donc à une lettre d'information qui agace ses lecteurs de ralentir la réinitialisation d'un mot de passe.

Enfin, il faut choisir où le courrier réside. Exploiter un serveur de messagerie implique du stockage, du filtrage antipourriel, des correctifs et une réputation d'expéditeur à gagner puis à conserver. La réponse habituelle associe une boîte hébergée pour la lecture à un prestataire d'envoi pour les messages automatiques. Ce choix mérite d'être délibéré plutôt que laissé aux réglages initiaux.

À quoi cela ressemble en pratique

Sur une plateforme, le courrier assurait les vérifications, les notifications, les récapitulatifs et les campagnes ; le recours à un prestataire unique rendait chaque interruption totale. La réponse a consisté à placer trois prestataires derrière une seule interface avec bascule automatique : SendGrid d'abord, puis SMTP2GO et Azure Communication Services. Des webhooks entrants rapportent ce que chaque prestataire a fait d'un message. Les deux côtés de l'échange sont consignés dans un journal d'envoi et une table d'événements de distribution : le statut de distribution communiqué par le prestataire peut donc être consulté plutôt que supposé. Les campagnes destinées à des segments d'utilisateurs reposent sur un schéma de diffusion distinct de 5 tables et 24 fonctions, construit à part du courrier transactionnel parce que le problème est différent. Un contrôle au démarrage envoie un vrai message à travers toute la chaîne lorsqu'un indicateur l'active. En développement, son échec produit un avertissement dans les journaux ; en préproduction et en production, il arrête le processus. La page indique aussi le coût : trois intégrations à maintenir et des journaux de distribution qui grossissent et doivent être purgés.

Le courrier de l'entreprise commence dans le DNS. Sa zone contient une vingtaine d'enregistrements, dont l'acheminement du courrier par un prestataire de boîtes hébergées, un domaine d'envoi transactionnel et les enregistrements d'authentification des deux. La zone entière est conservée sous forme de données dans le dépôt et réconciliée avec l'API du prestataire. Un point d'entrée d'audit rapporte l'écart entre la déclaration et ce qui est servi, sans rien modifier. C'est la partie la plus utilisée.

L'emplacement du courrier de l'entreprise a été décidé par le calcul. Ses services accessibles au public fonctionnent sur un hôte doté de 512 Mo de mémoire. Le courrier reste délibérément ailleurs : un serveur de messagerie demande une marge de ressources que cet hôte a déjà consommée. Il existe donc sous la forme d'un squelette d'installation en attente d'un hôte qui lui soit propre. En attendant, les messages adressés à l'entreprise sont lus dans sa propre boîte, hébergée chez Apple iCloud, sans liste de diffusion derrière elle.

Où les problèmes surviennent

Les messages commencent à arriver dans les indésirables la semaine où le prestataire change. Rien n'a changé dans l'application, mais les serveurs destinataires deviennent méfiants. Les enregistrements publiés par le domaine désignent encore l'ancien expéditeur ; les messages du nouveau arrivent donc sans signature ou depuis un hôte que le domaine n'a jamais autorisé. Ajoutez le nouvel expéditeur aux enregistrements avant la bascule, conservez l'ancien jusqu'au départ de son dernier message et, si le domaine en demande, lisez les rapports agrégés renvoyés par les serveurs destinataires.

L'application démarre, mais personne ne reçoit rien. Une clé expirée ou un compte d'envoi suspendu ressemble exactement à une configuration qui fonctionne, jusqu'à ce qu'une personne attende un code. Envoyez un vrai message au démarrage partout où le silence est dangereux et consignez ce que le prestataire déclare pour chaque message : un courriel manquant doit pouvoir être retracé, plutôt que devenir un sujet de débat.

Les rejets s'accumulent à une adresse que personne ne lit. L'adresse de retour de l'enveloppe pointe vers une boîte `no-reply` ; les notifications d'échec permanent y arrivent sans être ouvertes. L'expéditeur continue d'écrire à des boîtes fermées depuis un an, ce que les serveurs destinataires interprètent

comme une habitude de spammeur. Faites pointer l'adresse de retour vers un système qui traite ces rapports et cessez d'envoyer à une adresse après un échec permanent.

Un refus temporaire est traité comme définitif. Les réponses SMTP commençant par 4 signifient de réessayer plus tard ; celles commençant par 5 signifient d'arrêter. Un expéditeur qui abandonne au premier 4xx perd des messages qu'un serveur occupé ou prudent aurait acceptés une demi-heure plus tard. La RFC 5321 demande d'espacer les tentatives d'au moins 30 minutes et de ne pas abandonner avant au moins quatre à cinq jours. Le courrier transactionnel demande généralement des tentatives initiales plus rapprochées, puis un espacement croissant, ainsi qu'une trace claire de l'abandon définitif.

Pour aller plus loin

- RFC 5322 : format des messages Internet — les champs d'en-tête, la ligne vide, les limites de longueur des lignes et les deux champs obligatoires dans chaque message.
- RFC 5321 : protocole simple de transfert de courrier — l'enveloppe, les codes de réponse, la recherche des serveurs d'échange et les conseils sur les nouvelles tentatives.
- RFC 7208 : Sender Policy Framework (SPF) — la déclaration, par un domaine, des hôtes autorisés à envoyer du courrier en son nom.
- RFC 6376 : signatures DomainKeys Identified Mail (DKIM) — la signature des en-têtes et du corps avec une clé que le destinataire récupère dans le DNS.
- RFC 7489 : DMARC — le lien entre les deux contrôles et le domaine `From:` visible, avec une politique et des rapports ; un document informatif plutôt qu'une norme.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le processus de travail, les interfaces existantes et les utilisateurs qui ont besoin du changement. Nous pouvons définir une livraison testable et une transmission permettant à votre équipe d'assurer la maintenance des éléments livrés.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce qu'un courriel ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/email/