Les Mails

PAR RIONER & LITEAPP

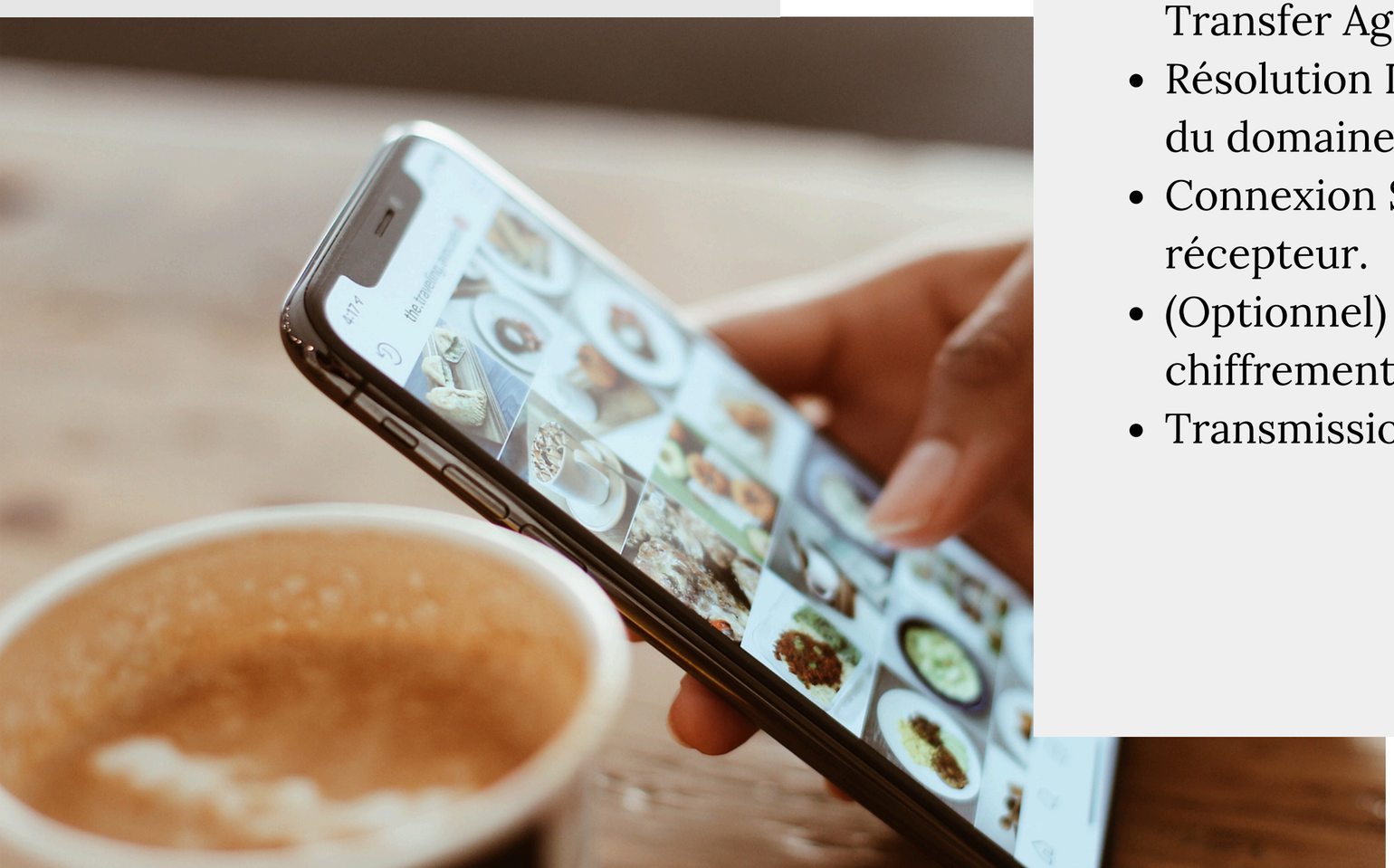
Sommaire

1. L’objet
2. Introduction
3. Le contenu
4. Bye bye

La vraie forma

1. Envoyer un mail
2. Recevoir un mail
3. À MiNET
4. TP Check Mark

Envoyer un mail



Je clique sur **envoyer**, puis :

- Connexion de mon ordinateur à mon MTA (Mail Transfer Agent)
- Résolution DNS du serveur MX (Mail Exchanger) du domaine destinataire.
- Connexion SMTP entre MTA expéditeur et MX récepteur.
- (Optionnel) Négociation STARTTLS et chiffrement TLS.
- Transmission et réception du message via SMTP.

Le protocole SMTP

```
E → M : MAIL FROM:<alexis@example.com>
M → R : TCP connexion vers R:25

R → M : 220 mail.receiver.net ESMTP Postfix
M → R : EHLO mail.example.com
R → M : 250-mail.receiver.net Hello
          250-STARTTLS
          250-AUTH
          250 OK
M → R : STARTTLS
R → M : 220 Ready to start TLS

// Tout le délire d’échandes de clés toussa toussa

M → R : EHLO mail.example.com
R → M : 250-mail.receiver.net Hello
          250-AUTH
          250 OK
M → R : MAIL FROM:<alexis@example.com>
R → M : 250 OK

M → R : RCPT TO:<destinataire@receiver.net>
R → M : 250 OK
M → R : DATA
R → M : 354 End data with <CR><LF>.<CR><LF>
M → R :
From: Alexis <alexis@example.com>
To: Destinataire <destinataire@receiver.net>
Subject: Test SMTP sécurisé
Date: Mon, 28 Apr 2025 10:15:00 +0200
Message-ID: <abc123@example.com>
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; s=default;
 h=from:to:subject:date;
 bh=47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=;
 b=abcDEFghiJKLmnOPqrSTUvwxYZ1234567890==

Bonjour Crocodilo Bombarilo,
tum tum tum tum sahur
Cordialement,
Alexis

.
R → M : 250 OK : queued as ABC123
M → R : QUIT
R → M : 221 Bye
```

VOYONS ENSEMBLE

La structure

Le mail en lui-même est composé de plusieurs parties :

Un des types de corps est multipart/signed, ce type permet de s’assurer de l’intégrité du message avec un certificat. Les messages de ce type affichent un tick à côté du nom de l’émetteur si le certificat est signé par un “root CA” de confiance

Enveloppe SMTP

MAIL FROM, RCPT TO

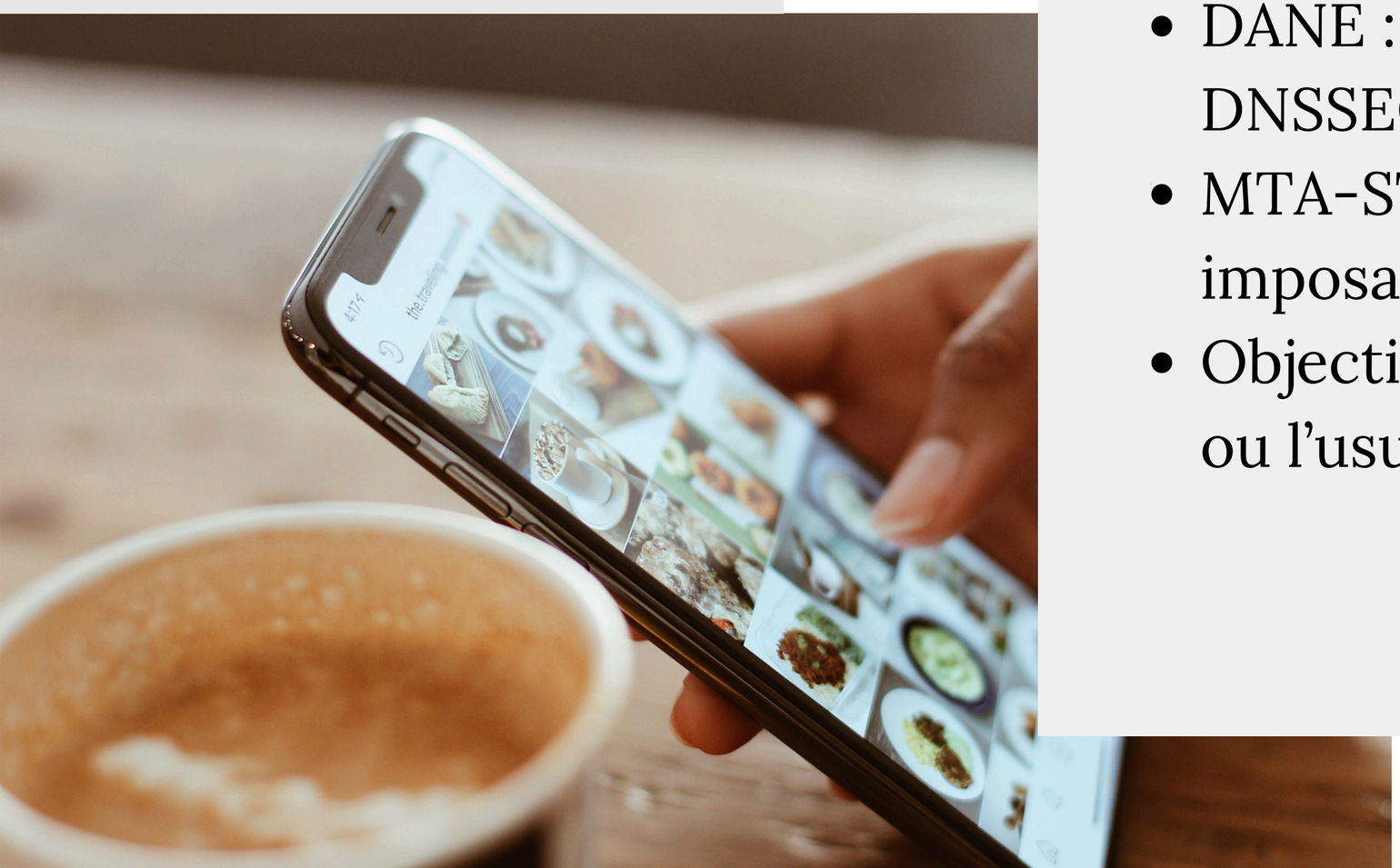
En-têtes (Headers) :

- From, To, Subject, Date, Message-ID
- Optional : Reply-To, CC, BCC
- Authentification : DKIM, SPF, Received

Corps (Body) :

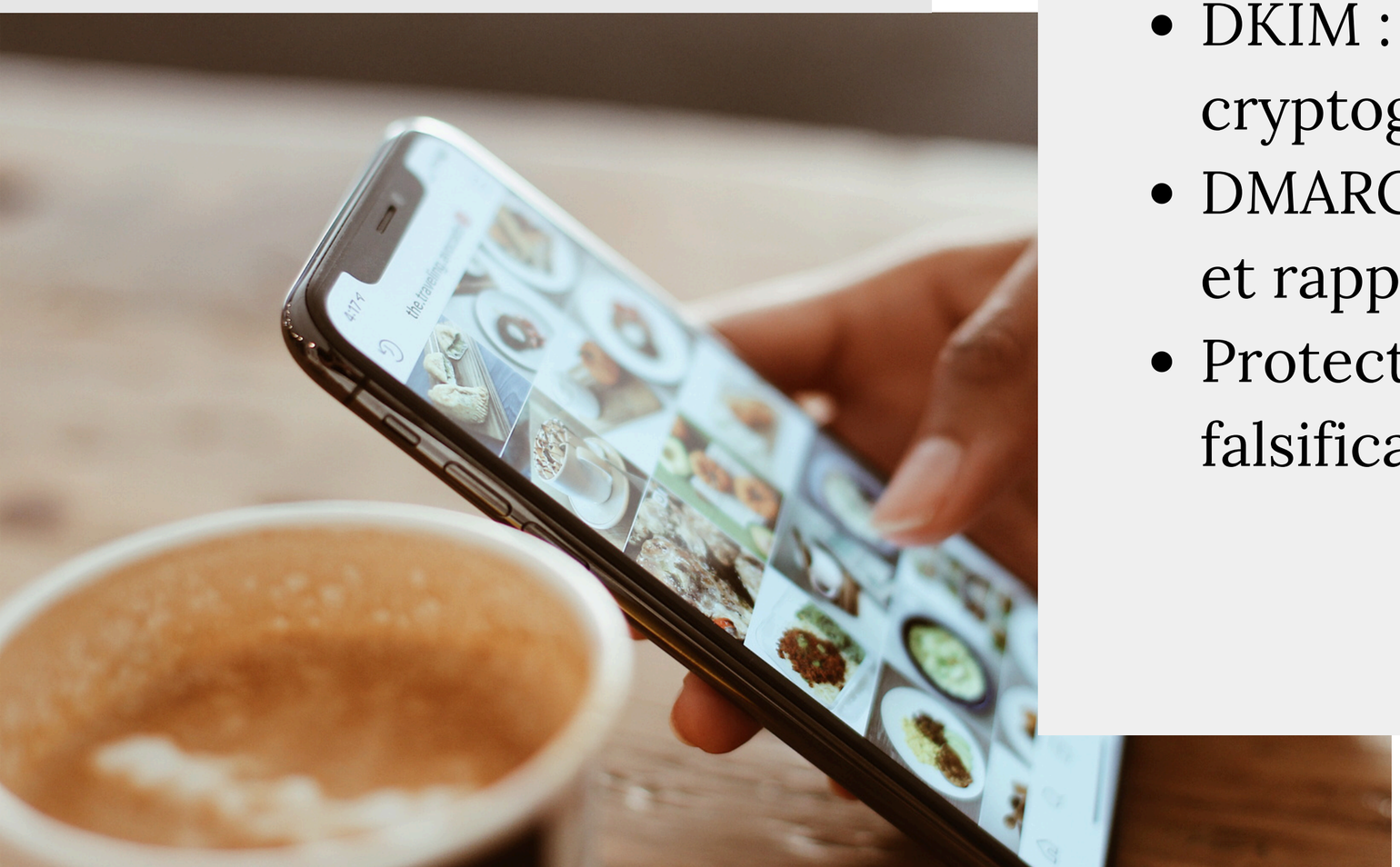
- Texte brut ou MIME multipart (HTML, pièces jointes)
- Encodage (Base64, Quoted-Printable)

Sécuriser l’envoi



- STARTTLS : conversion de la connexion SMTP en TLS.
- DANE : validation du certificat via DNSSEC + TLSA.
- MTA-STS : politique HTTPS imposant le TLS et validant le MX.
- Objectif : empêcher l’interception ou l’usurpation du serveur MX.

Sécuriser la réception



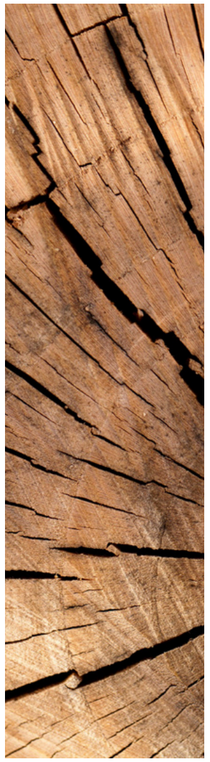
- SPF : autorise les IP à envoyer pour un domaine.
- DKIM : signature cryptographique des mails.
- DMARC : politique d’alignement et rapports de conformité.
- Protection contre le phishing et falsification d’adresse.

Recevoir un mail

Avec POP
(Post Office Protocol)

- Connexion directe au serveur POP (port 110 ou 995).
- Récupération et suppression locale des messages.
- Pas de synchronisation entre plusieurs appareils.
- Gestion limitée : uniquement la boîte de réception.



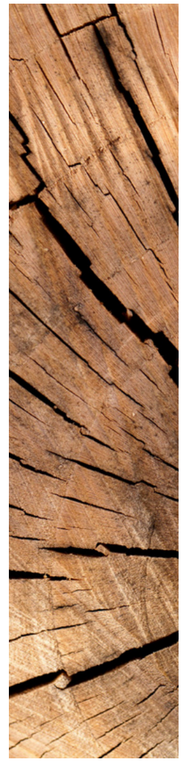


Recevoir un mail

Avec IMAP
(Internet Message Access Protocol)

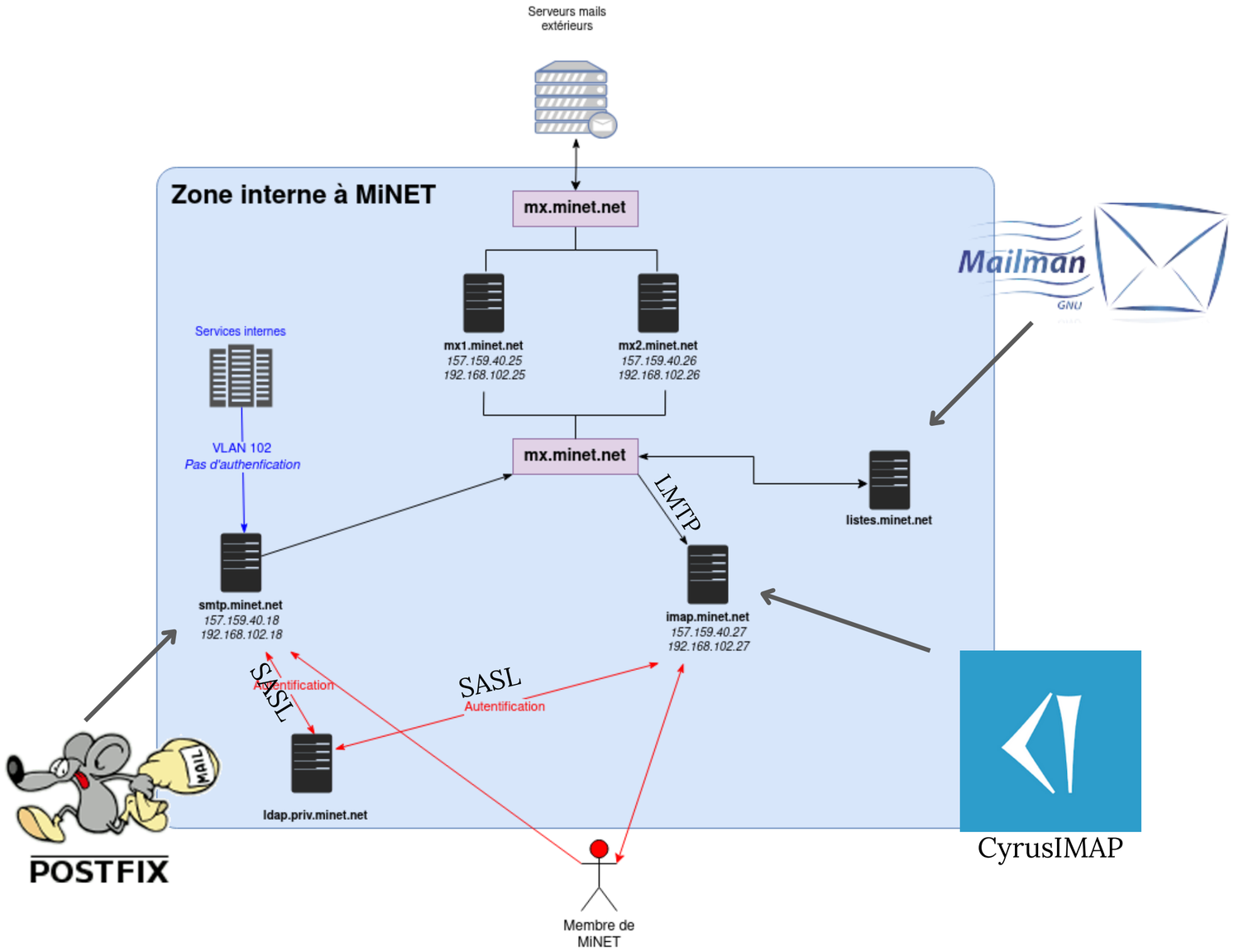
- Consultation et gestion des mails sur le serveur (port 143 ou 993).
- Synchronisation des dossiers et statuts entre appareils.
- Messages stockés sur le serveur, accessibles à la demande.
- Gestion complète : dossiers, états (lu, non lu…), suppression à distance.





COMMENT ON FAIT

à MiNET

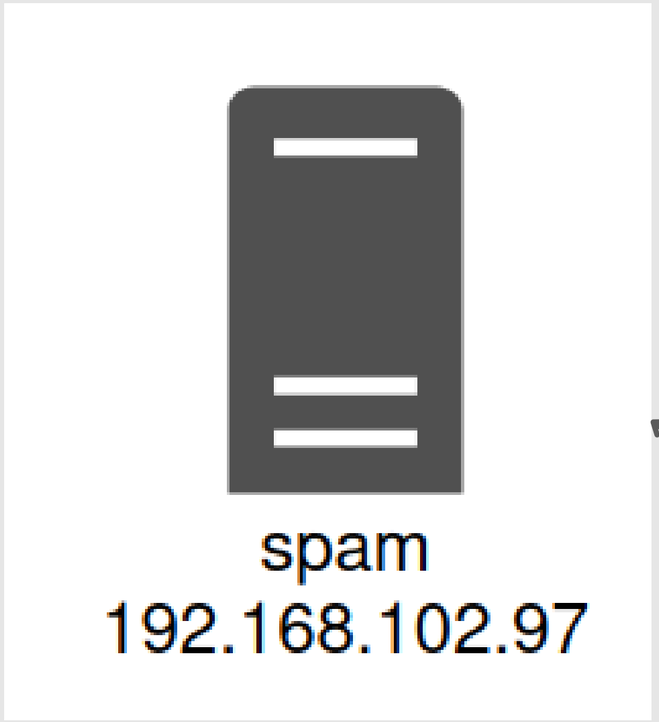


COMMENT ON FAIT

à MiNET

COMMENT ON FAIT

contre le spam ?



ClamAV
(antivirus)

SpamAssassin
(antispam)

Amavis

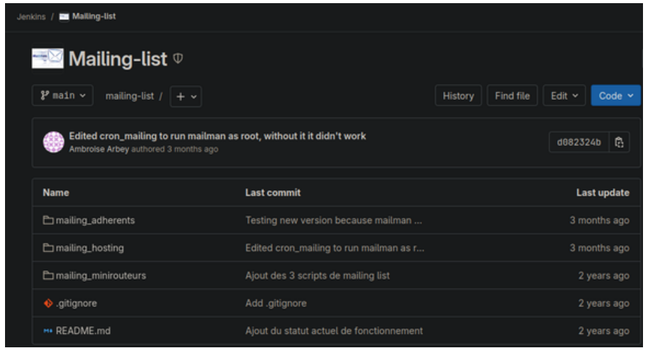
COMMENT ON FAIT

pour envoyer à beaucoup de gens ?

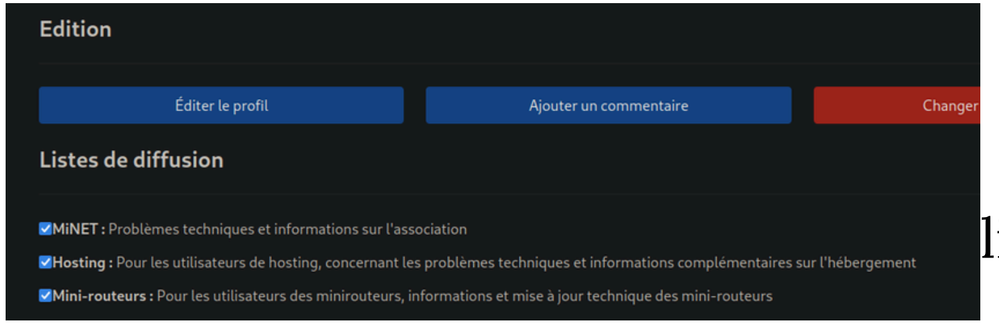
Gestion de tout ce qui a à voir avec les listes (en gros)

Postorius
interface graphique
de Mailman

Hyperkitty
interface graphique
(archivage)



Des scripts cool
(génération automatique
de mailing lists)



adh6
pour quelques
listes particulières

TP COMMENT ENVOYER DES MAILS PREMIUM

AVRIL 2025

SPONSORISÉ PAR S/MIME

Les étapes

1. ACTALIS.COM
2. CRÉEZ UN COMPTE
3. PRODUCTS > S/MIME
4. SUIVEZ LES ÉTAPES
5. ATTENDRE UN PEU

Importer le certificat

SUR WINDOWS & MACOS

Windows :

```
certutil -p "mdp_reçu_par_mail" -importpfx "C:
\path.p12"
```

MacOS :

```
security import /path/to/certificate.p12 -k ~/Library/
Keychains/login.keychain-db -P "mdp_reçu_par_mail" -T
/System/Applications/Mail.app
```

Evolution

POUR LES CHAD AVEC LINUX

- Ouvrir Evolution.
- Aller dans Édition > Préférences.
- Sélectionner votre compte e-mail dans la liste.
- Cliquer sur Modifier.
- Naviguer jusqu'à l'onglet Sécurité.
- Dans la section Certificats S/MIME :
- Pour Signer les messages, cliquer sur Sélectionner et choisir votre certificat.
- Pour Chiffrer les messages, cliquer sur Sélectionner et choisir le certificat correspondant.
- Cocher Signer numériquement les messages sortants par défaut

Outlook

APRÈS AVOIR EXÉCUTÉ LA COMMANDE

- Fichier > Options
- Centre de gestion de la confidentialité > Paramètres du Centre de gestion
- Sécurité des courriers électroniques
- Dans Certificats et algorithmes, cliquer sur Paramètres…
- Choisir le certificat de signature et le certificat de chiffrement
- Définir l’algorithme sur SHA256
- Cocher Signer par défaut

Apple Mail

APRÈS AVOIR EXECUTÉ LA COMMANDE

- Mail > Réglages > Comptes
- Sélectionner le compte
- Onglet Informations du compte
- Section Sécurité
- Choisir le certificat de signature et le certificat de chiffrement
- Cocher Signer par défaut