3. Https avec certificat signé gratuit

Cette configuration n'est pas conseillée sauf si vous ou votre prestaire informatique maitrisez l'utilisation sou Linux des composantes pour la gestion d'un certificat **Let's Encrypt** (Let's Encrypt est une autorité de certification (CA) gratuite qui délivre des certificats SSL/TLS permettant d'activer le HTTPS sur un site web.

La gestion d’un certificat **HTTPS Let's Encrypt** est généralement **automatisée** :

1. **Demande du certificat** auprès de Let's Encrypt via un client (ex. **Certbot**, **acme.sh**, **Caddy**, **Traefik**).
2. **Validation du domaine** (challenge ACME HTTP-01, DNS-01 ou TLS-ALPN-01).
3. **Installation du certificat** sur le serveur web (Nginx, Apache, IIS, proxy, etc.). Utiliser le service
4. **Renouvellement automatique** tous les 60 à 90 jours (Let's Encrypt délivre des certificats valides 90 jours).
5. **Rechargement du service web** après renouvellement pour prendre en compte le nouveau certificat.
6. **Supervision** de l’expiration et des éventuelles erreurs de renouvellement.

En résumé : un agent ACME installé sur le serveur obtient, renouvelle et déploie automatiquement le certificat Let's Encrypt sans intervention manuelle.

L'esnemble de cette mise en oeuvre est sous la responsabilité du client ou de son prestataire.

Revision #3
Created 13 May 2026 16:45:48 by Jacques LEGAT
Updated 2 July 2026 15:41:16 by Jacques LEGAT