Vladimir Spirine

Préconisations sur la configuration du mail

Table des matières

1. Contexte et périmètre

Dans le cadre de sa mission de suivi vaccinal, la plateforme MesVaccins / Colibri traite quotidiennement des échanges électroniques avec de nombreux acteurs de santé : Agences Régionales de Santé (ARS), établissements scolaires, structures médico-sociales et professionnels partenaires.
Le courriel constitue un vecteur essentiel pour la communication, la création de comptes, la gestion des accès et la transmission d'informations sensibles.

Trois types d'emails sont actuellement utilisés :

Transactionnels : création ou récupération de compte, réinitialisation de mot de passe, confirmation de rendez-vous, notifications de carnet.

Support : échanges techniques et administratifs via Google Workspace (Gmail).

Campagnes / Information : envois massifs à destination des établissements partenaires via Brevo (Sendinblue), Mailgun (UE) et Amazon SES.

L'objectif de cet audit est double :

Renforcer la sécurité des envois d'emails pour prévenir toute tentative de spoofing ou d'usurpation d'identité numérique.

Améliorer la délivrabilité et la conformité réglementaire (RGPD et HDS) en durcissant les mécanismes d'authentification — SPF, DKIM, DMARC — ainsi que les protocoles de transport sécurisés (TLS, MTA-STS, TLS-RPT).

L'audit repose sur l'analyse des enregistrements DNS, des en-têtes d'emails réels et des politiques de sécurité applicables à chaque flux d'envoi.

---

2. Résumé exécutif

Les contrôles réalisés mettent en évidence une infrastructure d'emailing globalement saine et maîtrisée, reposant sur des prestataires reconnus (Google, Mailgun, Amazon).
Cependant, plusieurs axes d'amélioration sont nécessaires pour atteindre un niveau de sécurité conforme aux pratiques du secteur de la santé.

Principaux constats

SPF : enregistrement valide, couvrant les trois prestataires, mais trop permissif (~all).

DKIM : signature correcte côté Google Workspace (sélecteur 20230601), non homogène sur l'ensemble des routes d'envoi.

DMARC : présent, mais configuré en mode observation (p=none), donc sans action préventive contre les emails falsifiés.

Recommandation prioritaire

Mettre en œuvre une montée en puissance progressive de la politique DMARC vers p=reject, accompagnée d'une industrialisation des signatures DKIM, d'un nettoyage du SPF et de l'ajout des dispositifs MTA-STS / TLS-RPT pour sécuriser le transport des courriels.

---

3. Inventaire et éléments analysés

3.1 Enregistrements DNS relevés

Nom	Type	Valeur
mesvaccins.net	TXT	v=spf1 include:_spf.google.com include:eu.mailgun.org include:amazonses.com ~all
_dmarc.mesvaccins.net	TXT	v=DMARC1; p=none; rua=mailto:rua@dmarc.brevo.com
Divers	TXT	google-site-verification=… ; brevo-code=… ; stripe-verification=…

3.2 Extrait d'un message signé (Gmail)

Domaine : mesvaccins-net.20230601.gappssmtp.com

Sélecteur : 20230601

Résultat DKIM : pass

Résultat SPF : pass (via include Google)

Observation : SPF_HELO_NONE → absence de SPF pour le nom HELO du serveur relai.

Score antispam : faible, aucun indicateur de spam détecté.

---

4. Analyse technique et interprétation

4.1 SPF (Sender Policy Framework)

Le mécanisme SPF permet de définir, au niveau DNS, les serveurs autorisés à envoyer des emails au nom du domaine.

L’enregistrement SPF actuel est fonctionnel et inclut correctement les prestataires Google, Mailgun (Europe) et Amazon SES.

Forces identifiées :

Couverture complète des principaux canaux d’envoi.

Configuration conforme aux standards.

Risques et points d’attention :

Trop grand nombre d’include → risque de dépasser la limite des 10 requêtes DNS (RFC 7208).

Mécanisme final ~all (softfail) : permissif, autorisant temporairement des serveurs non listés.

SPF_HELO_NONE signale une absence de politique côté HELO, à corriger pour une cohérence totale.

Évaluation : conformité basique, à renforcer pour un domaine manipulant des données de santé.

4.2 DKIM (DomainKeys Identified Mail)

Le protocole DKIM signe numériquement chaque message. Il garantit que le contenu n’a pas été modifié et que l’expéditeur est bien authentifié.

Constat :

Signature valide via Google Workspace (sélecteur 20230601).

Pas de validation confirmée pour Mailgun et Amazon SES.

Longueur de clé correcte (≥1024 bits), mais passage à 2048 bits recommandé.

Recommandations :

Publier une clé DKIM distincte par prestataire et par usage (support@, no-reply@, notifications@).

Mettre en place une rotation semestrielle des clés.

Tenir un registre de suivi des sélecteurs avec dates et responsables.

Activer la signature systématique sur tous les flux sortants.

4.3 DMARC (Domain-based Message Authentication, Reporting & Conformance)

DMARC permet de définir la politique d'acceptation ou de rejet des emails en fonction des résultats SPF et DKIM, et d'obtenir des rapports d'analyse.

Configuration actuelle :

v=DMARC1; p=none; rua=mailto:rua@dmarc.brevo.com

Mode « observation » sans action corrective.

Alignement par défaut en mode « relaxed ».

Analyse :
Ce mode est utile en phase initiale, mais n'empêche pas la falsification d'emails. Pour un domaine manipulant des données de santé, une politique bloquante (p=reject) est impérative à moyen terme.

Recommandations :

Passer progressivement à p=quarantine, puis p=reject.

Forcer l'alignement strict : adkim=s; aspf=s.

Définir une adresse de rapports « forensic » dédiée : ruf=mailto:ruf@mesvaccins.net.

---

5. Recommandations globales

5.1 Politique DMARC – montée en puissance

Étape initiale :
p=quarantine; pct=10; adkim=s; aspf=s; fo=1; rua=mailto:rua@dmarc.brevo.com; ruf=mailto:ruf@mesvaccins.net

Suivi des rapports pendant 2 à 4 semaines, augmentation progressive de pct.

Passage final à p=reject avec ajout de sp=reject pour les sous-domaines.

Stockage et analyse régulière des rapports (Brevo, SIEM interne).

5.2 SPF – rationalisation et durcissement

Retirer tout prestataire inactif.

Vérifier que le nombre de requêtes DNS reste <10.

Publier un SPF pour chaque domaine HELO utilisé.

Passer à -all une fois DMARC stabilisé.

Documenter la configuration de chaque route d'envoi.

5.3 DKIM – industrialisation

Utiliser un sélecteur par prestataire :

20230601._domainkey (Google)

mg1._domainkey (Mailgun)

ses1._domainkey (Amazon SES)

Rotation semestrielle des clés.

Vérification publique de la clé et cohérence des signatures.

Maintenir un référentiel des clés DKIM actives.

5.4 Sécurité du transport

Déployer MTA-STS pour imposer le chiffrement TLS entre serveurs de messagerie.

Publier un fichier /.well-known/mta-sts.txt en mode enforce.

Ajouter TLS-RPT pour la remontée des échecs TLS.

Vérifier la cohérence FCrDNS (PTR ↔ HELO).

Mettre en place ARC sur les relais afin de préserver la chaîne d'authentification.

Ajouter un en-tête List-Unsubscribe pour les communications massives.

5.5 Conformité RGPD et HDS

Interdire toute donnée médicale dans les objets ou contenus non chiffrés.

Utiliser S/MIME pour les échanges sensibles.

Restreindre les accès aux rapports DMARC/TLS-RPT (accès nominatif, durée de conservation limitée).

Héberger les données sur des serveurs conformes HDS.

5.6 Suivi et indicateurs (KPIs)

Centraliser les rapports DMARC via Brevo.

Utiliser Google Postmaster Tools, Mailgun Dashboard et SES Console.

Suivre les indicateurs clés :

taux d'alignement SPF/DKIM,

réputation du domaine,

taux de plaintes (<0,1 %),

délivrabilité,

taux de rebonds.

Intégrer ces données dans un tableau de bord cybersécurité mensuel.

---

6. Feuille de route – déploiement sur 6 semaines

Semaine	Actions principales
1	Cartographie des routes d'envoi, validation DKIM par prestataire
2	Activation de DMARC (p=quarantine; pct=10) + MTA-STS/TLS-RPT
3–4	Augmentation progressive du pourcentage (50 → 100), rotation DKIM
5	Passage en p=reject + ajout sp=reject
6	Revue KPI, documentation finale et mise en routine mensuelle

---

7. Exemples d'enregistrements DNS cibles

DMARC (phase intermédiaire)
_dmarc.mesvaccins.net TXT "v=DMARC1; p=quarantine; pct=50; adkim=s; aspf=s; fo=1; rua=mailto:rua@dmarc.brevo.com; ruf=mailto:ruf@mesvaccins.net; sp=quarantine"

MTA-STS
_mta-sts.mesvaccins.net TXT "v=STSv1; id=20251024"
Contenu :

version: STSv1

mode: enforce

mx: *.mesvaccins.net

max_age: 86400

TLS-RPT
_smtp._tls.mesvaccins.net TXT "v=TLSRPTv1; rua=mailto:tlsrpt@mesvaccins.net"

SPF (version durcie)
mesvaccins.net TXT "v=spf1 include:_spf.google.com include:eu.mailgun.org include:amazonses.com -all"

---

8. Plan de validation

Envoi de tests vers dkimvalidator.com, Gmail et Outlook.com.

Vérification : SPF = pass / DKIM = pass / DMARC = pass et aligné.

Analyse des rapports DMARC et TLS-RPT pendant 30 jours.

Simulation d'un spoof : attendu → rejet ou quarantaine.

Revue finale des indicateurs de délivrabilité.

---

9. Lexique technique (abrégé)

Terme	Définition synthétique
SPF	Définit les serveurs autorisés à envoyer des emails pour un domaine.
DKIM	Signature numérique garantissant l'intégrité du message.
DMARC	Politique d'authentification combinant SPF et DKIM.
MTA-STS / TLS-RPT	Protocoles de sécurité du transport chiffré et de reporting.

Terme	Définition synthétique
ARC	Conserve la traçabilité d'authentification en cas de transfert.
HELO / PTR	Identifiants SMTP du serveur, utilisés pour la vérification DNS.
S/MIME	Chiffrement et signature des emails professionnels.
RGPD / HDS	Réglementations relatives à la protection des données de santé.
rua / ruf	Adresses de réception des rapports DMARC (agrégés et forensic).
p=none / quarantine / reject	Niveaux de politique DMARC (observation → rejet).

Conclusion

La plateforme MesVaccins / Colibri dispose déjà d'une infrastructure email solide, mais son durcissement est indispensable pour atteindre le niveau d'exigence attendu dans le secteur de la santé.
Le plan proposé — articulé autour de la montée en puissance DMARC, de la généralisation DKIM, et du déploiement MTA-STS/TLS-RPT — permettra d'assurer une authentification forte, une réduction significative du risque de spoofing, et une conformité RGPD / HDS durable.