SP

# SpoofProof

## Constat d'authentification email

données DNS publiques

DOMAINE AUDITÉ
**example.com**

DATE ET HEURE D'AUDIT
**4 août 2026 à 14:08 UTC**

### Mention de périmètre

Ce rapport présente un constat à partir de données DNS publiques, de la politique MTA-STS publiée le cas échéant et du certificat TLS public du domaine. Aucun test intrusif, aucune connexion SMTP et aucun envoi d'email ne sont réalisés.

Document d'exemple généré automatiquement depuis le moteur d'audit SpoofProof.

# Synthèse exécutive



SCORE REPRIS DU MOTEUR

**70**/100

CORRECT

MESSAGE IMPOSÉ PAR LE BARÈME

**La configuration bloque l'usurpation dans la majorité des cas**

Version barème: 2026-08-04-fixed-email-auth-v1

## Résumé en langage clair

- Le score repris du moteur d'audit est 70/100, niveau Correct.
- Le constat s'appuie uniquement sur les données DNS publiques et sur le certificat TLS public du domaine example.com.
- Les points à examiner en priorité sont: DKIM non confirmé sur les sélecteurs testés, MTA-STS enforce non observé, TLS-RPT non observé, rapports DMARC non renseignés.
- Ce document sert de base de décision: il ne remplace pas une revue interne des outils qui envoient effectivement des emails.

### Limite d'interprétation

Le score, le niveau et le message ci-dessus sont repris tels quels depuis le moteur d'audit. Le rapport ne les recalcule pas et ne les arrondit pas.

# Détail par contrôle



## SPF

BLOCAGE SPF STRICT

CONSTAT

Enregistrement: v=spf1 -all. Mécanisme final: -all. Résolutions induites: 0/10.

IMPLICATION CONCRÈTE

Le domaine annonce quels serveurs peuvent émettre des emails pour lui. Un mécanisme final souple laisse plus de tolérance aux expéditeurs non prévus.

## DKIM

NON CONCLU SUR LES SÉLECTEURS TESTÉS

CONSTAT

aucun sélecteur parmi ceux testés n'a répondu, ce qui ne prouve pas l'absence de DKIM

IMPLICATION CONCRÈTE

Le test ne permet pas de confirmer la signature DKIM utilisée en production; une vérification avec le prestataire email reste nécessaire.

## DMARC

POLITIQUE REJECT

CONSTAT

Enregistrement: v=DMARC1;p=reject;sp=reject;adkim=s;aspf=s. Politique domaine: reject. Sous-domaines: reject. Rapports: non renseignés.

IMPLICATION CONCRÈTE

DMARC indique aux destinataires comment traiter les messages qui ne passent pas les contrôles SPF/DKIM alignés.

# Détail par contrôle



## Alignement SPF/DKIM

ALIGNEMENT STRICT

CONSTAT

SPF: strict. DKIM: strict.

IMPLICATION CONCRÈTE

L'alignement détermine si le domaine visible par le client correspond au domaine validé par SPF ou DKIM.

## MX et cohérence SPF

MX OBSERVÉS · COHÉRENCE UNKNOWN

CONSTAT

Serveurs MX: {"exchange":"","priority":0}. Impossible d'évaluer la cohérence: prestataire SPF ou MX non reconnu.

IMPLICATION CONCRÈTE

La cohérence entre les serveurs de réception et les prestataires déclarés dans SPF aide à repérer les configurations dispersées.

## MTA-STS

MTA-STS ENFORCE NON OBSERVÉ

CONSTAT

Aucun enregistrement MTA-STS TXT observé. URL testée: https://mta-sts.example.com/.well-known/mta-sts.txt.

IMPLICATION CONCRÈTE

MTA-STS publie une politique de transport SMTP chiffré pour les serveurs qui la consultent.

# Détail par contrôle



## TLS-RPT

TLS-RPT NON OBSERVÉ

CONSTAT

Aucun enregistrement _smtp._tls n'a été observé.

IMPLICATION CONCRÈTE

TLS-RPT permet de recevoir des rapports agrégés sur les problèmes de transport email chiffré.

## DNSSEC

DS OBSERVÉ

CONSTAT

Enregistrements DS: {"name":"example.com","ttl":86125,"type":43,"data":"2371 ECDSAP256SHA256 2 c988ec423e3880eb8dd8a46fe06ca230ee23f35b578d64e78b29c3e1c83d245a"}.

IMPLICATION CONCRÈTE

DNSSEC donne aux résolveurs compatibles un moyen de vérifier l'intégrité des réponses DNS publiées.

## Certificat TLS public

CERTIFICAT VALIDE OBSERVÉ

CONSTAT

Hôte: example.com:443. Sujet: example.com. Émetteur: Cloudflare TLS Issuing ECC CA 3. Expiration: Oct 27 22:17:21 2026 GMT (84 jours).

IMPLICATION CONCRÈTE

Ce contrôle concerne le certificat HTTPS public du domaine, utile pour la cohérence externe du constat.

# Recommandations priorisées



Actions classées par impact attendu, formulées pour arbitrage métier. Les corrections techniques doivent être validées avec le prestataire email/DNS avant mise en production.

| | | | |
|---|---|---|---|
| 01 | IMPACT FORT | **Confirmer DKIM avec le prestataire email** | aucun sélecteur parmi ceux testés n'a répondu, ce qui ne prouve pas l'absence de DKIM. Récupérer les sélecteurs réels et ajouter les clés nécessaires si elles manquent. |
| 02 | IMPACT MOYEN | **Ajouter une adresse de rapports DMARC** | Recevoir les rapports agrégés permet de suivre les sources d'envoi et les rejets au fil du temps. |
| 03 | IMPACT MOYEN | **Déployer MTA-STS en mode enforce** | Publier l'enregistrement TXT et la politique HTTPS une fois les MX confirmés. |
| 04 | IMPACT COMPLÉMENTAIRE | **Ajouter TLS-RPT** | Publier _smtp._tls pour recevoir des rapports sur les erreurs de transport email chiffré. |
| 05 | GOUVERNANCE | **Conserver ce constat avec la date d'audit** | Rejouer le contrôle après correction puis à chaque changement de prestataire email ou DNS. |

# Annexe — preuves brutes



Extrait des réponses archivées par le moteur au moment du constat. Les valeurs longues sont raccourcies dans cette annexe PDF; le JSON d'audit conserve la structure brute complète.

| | | |
|---|---|---|
| 4 août 2026 à 14:08 UTC | **TXT example.com**<br>Serveur: 172.21.0.1, 1.1.1.1, 8.8.8.8 | `[["v=spf1 -all"], ["_k2n1y4vw3qtb4skdx9e7dxt97qrmmq9"]]` |
| 4 août 2026 à 14:08 UTC | **MX example.com**<br>Serveur: 172.21.0.1, 1.1.1.1, 8.8.8.8 | `[{"exchange":"","priority":0}]` |
| 4 août 2026 à 14:08 UTC | **TXT _dmarc.example.com**<br>Serveur: 172.21.0.1, 1.1.1.1, 8.8.8.8 | `[["v=DMARC1;p=reject;sp=reject;adkim=s;aspf=s"]]` |
| 4 août 2026 à 14:08 UTC | **TXT default._domainkey.example.com**<br>Serveur: 172.21.0.1, 1.1.1.1, 8.8.8.8 | `[["v=DKIM1; p="]]` |
| 4 août 2026 à 14:08 UTC | **TXT _mta-sts.example.com**<br>Serveur: 172.21.0.1, 1.1.1.1, 8.8.8.8 | `queryTxt ENODATA _mta-sts.example.com` |
| 4 août 2026 à 14:08 UTC | **TXT _smtp._tls.example.com**<br>Serveur: 172.21.0.1, 1.1.1.1, 8.8.8.8 | `queryTxt ENODATA _smtp._tls.example.com` |
| 4 août 2026 à 14:08 UTC | **TXT google._domainkey.example.com**<br>Serveur: 172.21.0.1, 1.1.1.1, 8.8.8.8 | `[["v=DKIM1; p="]]` |
| 4 août 2026 à 14:08 UTC | **CNAME mta-sts.example.com**<br>Serveur: 172.21.0.1, 1.1.1.1, 8.8.8.8 | `queryCname ENODATA mta-sts.example.com` |
| 4 août 2026 à 14:08 UTC | **? ?**<br>Serveur: example.com:443 | `{"subject":{"CN":"example.com"},"issuer":{"C":"US","O":"SSL Corporation","CN":"Cloudflare TLS Issuing ECC CA 3"},"validFrom":"Jul 29 22:10:08 2026 GMT","validTo":"Oct 27 22:17:21 2026 GMT","expiresInDays":84,"validNow":true,"authorizatio` |
| 4 août 2026 à 14:08 UTC | **TXT selector1._domainkey.example.com**<br>Serveur: 172.21.0.1, 1.1.1.1, 8.8.8.8 | `[["v=DKIM1; p="]]` |

### Traçabilité

Nombre total d'entrées archivées: 35. Serveurs DNS déclarés par le moteur: 172.21.0.1 ; 1.1.1.1 ; 8.8.8.8.