GUIDE TECHNIQUE

SPF, DKIM & DMARC Les Fondements de l'Authentification Email

Comprendre, configurer et maintenir
les protocoles d'authentification

DMARC EXPERT KFT

Votre partenaire de confiance en sécurité et délivrabilité email

contact@dmarc.fr | www.dmarc-expert.com

Pourquoi authentifier ses emails ?

L'email reste le **vecteur principal des cyberattaques**. Phishing, usurpation d'identité, fraude au président — toutes ces menaces exploitent la faiblesse fondamentale du protocole SMTP : n'importe qui peut envoyer un email en se faisant passer pour votre domaine. SPF, DKIM et DMARC constituent la réponse technique à cette vulnérabilité.

Obligation depuis 2024 : Gmail, Yahoo et Microsoft exigent SPF et DKIM pour tout expéditeur de masse. Sans authentification conforme, vos emails légitimes risquent d'être classés en spam ou définitivement rejetés.

SPF — Sender Policy Framework

SPF permet de déclarer dans le DNS la liste des serveurs autorisés à envoyer des emails pour votre domaine. Attention : un SPF mal configuré peut involontairement autoriser des sources malveillantes. DMARC EXPERT a audité des milliers d'enregistrements SPF et identifié des configurations risquées récurrentes.

- Maximum **10 résolutions DNS** — au-delà : erreur permerror
- Ne jamais utiliser **+all** (autorise tout) ni **?all** (neutre)
- Terminer par **-all** (reject) ou **~all** (softfail)
- Auditer régulièrement les **includes** tiers pour détecter les sources obsolètes

DKIM — DomainKeys Identified Mail

DKIM appose une **signature cryptographique** sur chaque email sortant. Le serveur destinataire vérifie cette signature via la clé publique publiée dans le DNS. Contrairement à SPF, DKIM résiste aux redirections et au forwarding. La gestion des clés DKIM multi-ESPs (Salesforce, Mailchimp, SAP, Oracle…) est l'une des complexités que DMARC EXPERT maîtrise.

- Utiliser des clés RSA de **2048 bits** minimum
- Renouveler les clés tous les **6 à 12 mois**
- Configurer DKIM pour chaque ESP tiers utilisé par l'organisation

DMARC — Domain-based Message Authentication, Reporting & Conformance

DMARC s'appuie sur SPF et DKIM pour définir la politique d'un domaine face aux emails non authentifiés. Il ajoute deux dimensions : les **rapports** (visibilité complète sur les flux email) et la **politique d'application**.

p=none	Surveillance uniquement — collecte de rapports, aucune action	Observation (J0→J30)
p=quarantine	Emails non conformes dirigés en spam / quarantaine	Transition (J30→J60)
p=reject	Emails non conformes rejetés définitivement par le destinataire	Enforcement (J60+)

Rapports DMARC & Intelligence Artificielle

DMARC génère des **rapports agrégés (RUA)** et **forensiques (RUF)**. La plateforme DMARC EXPERT transforme ces fichiers XML bruts en tableaux de bord lisibles. Les algorithmes d'IA embarqués détectent automatiquement les anomalies : nouveaux expéditeurs non déclarés, variations suspectes de volumes, tentatives d'usurpation, comportements inhabituels d'ESPs.

BIMI — Brand Indicators for Message Identification : une fois DMARC en p=reject, votre logo s'affiche automatiquement dans les boîtes de réception compatibles (Gmail, Yahoo, Apple Mail, Outlook…), renforçant la confiance et la reconnaissance de marque.