DKIM verstehen: Mail-Sicherheit clever steigern

Category: Online-Marketing
geschrieben von Tobias Hager | 10. Februar 2026

DKIM verstehen: Mail-Sicherheit clever steigern

Deine Marketing-Mails landen im Spam? Dein CRM schickt brav Kampagnen raus, aber keiner liest sie? Willkommen in der Welt ohne DKIM – dem digitalen Türsteher deiner E-Mails. Wer E-Mail-Marketing ohne DKIM betreibt, spielt russisches Roulette mit der Zustellbarkeit. Zeit, das kryptische Akronym endlich zu knacken – technisch, tief und ohne Bullshit.

- Was DKIM ist und warum es ein zentraler Bestandteil moderner E-Mail-Sicherheit ist
- Wie DKIM technisch funktioniert – mit Public Key, Private Key und DNS
- Warum DKIM allein nicht reicht und wie SPF und DMARC zusammenspielen
- Welche Tools dir helfen, DKIM korrekt zu implementieren und zu testen
- Was passiert, wenn DKIM fehlt oder falsch konfiguriert ist
- Wie du DKIM ganz konkret für deine Domain einrichtest – Schritt für Schritt
- Welche E-Mail-Provider DKIM unterstützen – und welche es verbocken
- Warum DKIM dein Retter im Spam-Krieg von 2025 ist

DKIM erklärt: Was DomainKeys Identified Mail eigentlich ist

DomainKeys Identified Mail, kurz DKIM, ist ein Authentifizierungsverfahren für E-Mails. Es sorgt dafür, dass der Empfänger deiner Mail sicher sein kann: Diese Nachricht stammt wirklich von dir – und nicht von einem windigen Spammer, der deinen Absender gefälscht hat. DKIM arbeitet mit kryptografischer Signatur und DNS-Records. Klingt komplex? Ist es auch. Aber ohne DKIM ist deine E-Mail praktisch nackt im digitalen Kugelhagel unterwegs.

Im Kern geht es bei DKIM darum, den Inhalt einer E-Mail digital zu signieren. Das geschieht mit einem sogenannten Private Key, der auf dem sendenden Server liegt. Der Empfänger kann über einen öffentlichen Schlüssel – den Public Key, der im DNS deiner Domain veröffentlicht wird – prüfen, ob die Signatur zur Domain passt und ob die Mail unterwegs manipuliert wurde. Wenn die Signatur validiert werden kann, steigt das Vertrauen – und damit die Chance, dass deine Mail den Posteingang erreicht.

Für Marketing, Transaktions-Mails und jedes andere E-Mail-basierte Geschäft ist DKIM keine Kür, sondern Pflicht. Ohne die Authentifizierung durch DKIM riskierst du nicht nur Zustellprobleme, sondern auch Reputationsschäden für deine Domain. Google, Microsoft und Apple werten fehlende oder fehlerhafte DKIM-Signaturen längst als Spam-Signal. Und das bedeutet: Deine Kampagne ist tot, bevor sie gelesen wurde.

Besonders kritisch: Viele Marketer verlassen sich auf ihre E-Mail-Dienstleister und haben keine Ahnung, ob DKIM korrekt eingerichtet ist. Spoiler: In vielen Fällen ist es das nicht. Und wenn du nicht selbst prüfst, ob deine DKIM-Keys aktiv und gültig sind, bist du einfach nur fahrlässig unterwegs.

Wie DKIM technisch

funktioniert – Public Key, Private Key und Header-Magie

DKIM basiert auf einem asymmetrischen Verschlüsselungsverfahren. Dabei kommen zwei Schlüssel zum Einsatz: der private Schlüssel (Private Key), den nur der sendende Server kennt, und der öffentliche Schlüssel (Public Key), der im DNS deiner Domain veröffentlicht wird. Die Idee: Der Absender signiert bestimmte Header-Felder der E-Mail mit dem Private Key. Der Empfänger kann mithilfe des Public Keys überprüfen, ob die Signatur korrekt ist und die Mail unterwegs nicht verändert wurde.

Die technische Umsetzung sieht so aus: Beim Versand der E-Mail werden bestimmte Header-Felder – zum Beispiel "From", "Subject" und "Date" – sowie der Body der Mail durch einen Hashing-Algorithmus (z. B. SHA-256) in einen einzigartigen Fingerabdruck verwandelt. Dieser Hash wird dann mit dem Private Key verschlüsselt – das ist die DKIM-Signatur. Diese Signatur wird im E-Mail-Header unter dem Feld "DKIM-Signature" mitgeschickt.

Der Empfänger-Server ruft nun über das DNS der Absender-Domain den Public Key ab. Dieser Key ist in einem speziellen TXT-Record im Format "selector._domainkey.domain.tld" hinterlegt. Mit diesem Schlüssel wird dann die Signatur überprüft. Passt alles – Glückwunsch, du hast bestanden. Passt sie nicht – willkommen im Spam-Ordner.

Ein typischer DKIM-Eintrag im DNS sieht so aus:

```
selector1._domainkey.example.com. IN TXT "v=DKIM1; k=rsa; p=MIGfMA0G...
(Public Key)"
```

Der "Selector" ist dabei ein frei wählbarer Identifier, der es erlaubt, mehrere DKIM-Schlüssel gleichzeitig zu verwenden – etwa bei Schlüsselrotationen oder unterschiedlichen Mail-Services. "_domainkey" ist das Standard-Präfix für DKIM-Einträge.

SPF, DKIM, DMARC: Das heilige Dreieck der E-Mail-Authentifizierung

Wer glaubt, DKIM alleine reicht, hat das große Bild nicht verstanden. Neben DKIM gibt es zwei weitere essentielle Technologien: SPF (Sender Policy Framework) und DMARC (Domain-based Message Authentication, Reporting and Conformance). Zusammen bilden sie das Rückgrat moderner E-Mail-Sicherheit – und nur im Zusammenspiel entfalten sie ihre volle Power.

SPF definiert, welche Server berechtigt sind, im Namen deiner Domain E-Mails zu versenden. Das wird ebenfalls über einen DNS-TXT-Record geregelt. Der Empfänger-Server prüft dann, ob die IP-Adresse des sendenden Mailservers im SPF-Record der Domain auftaucht. Ist das nicht der Fall, wird die Mail abgelehnt oder als verdächtig markiert.

DMARC wiederum ist die Policy-Schicht über SPF und DKIM. Hier definierst du, was passieren soll, wenn SPF oder DKIM fehlschlagen: nichts (none), markieren (quarantine) oder ablehnen (reject). DMARC liefert zusätzlich Reports, mit denen du sehen kannst, wer Mails in deinem Namen sendet – ein unschlagbares Tool zur Identifikation von Missbrauch und zur Kontrolle deiner E-Mail-Reputation.

Die ideale Konfiguration sieht so aus:

- SPF: korrekt gesetzter SPF-Record mit allen autorisierten Mailservern
- DKIM: gültige und funktionierende Signatur mit regelmäßig rotierenden Keys
- DMARC: Policy mit “reject” und aktiver Reporting-Adresse (ruf=mailto:…)

Nur wer alle drei Standards implementiert, kontrolliert wirklich die Authentizität seiner ausgehenden Mails – und schützt sich effektiv gegen Spoofing, Phishing und Blacklisting.

DKIM einrichten: So richtest du DKIM richtig ein (Step-by-Step)

Die Einrichtung von DKIM ist kein Hexenwerk, aber sie erfordert Präzision. Ein Tippfehler im DNS – und die Signatur schlägt fehl. Deshalb hier der ungeschönte Fahrplan zur korrekten Implementierung:

1. DKIM-Unterstützung prüfen
   Stelle sicher, dass dein E-Mail-Service-Provider (ESP) DKIM unterstützt. Bei Plattformen wie Mailchimp, Sendinblue, Mailgun oder Postmark findest du in der Regel eine Anleitung im Backend.
2. Selector und Schlüssel generieren
   Erstelle ein Schlüsselpaar (2048 Bit empfohlen). Die meisten ESPs generieren diese automatisch für dich. Du bekommst den Public Key als DNS-Eintrag und den Selector (z. B. “selector1”).
3. DNS-Eintrag setzen
   Logge dich bei deinem Domain-Registrar ein (z. B. IONOS, GoDaddy, Cloudflare) und füge einen neuen TXT-Record hinzu. Der Name lautet “selector._domainkey.deinedomain.de”, der Wert ist der Public Key.
4. Signatur aktivieren
   Aktiviere im Backend deines ESP die DKIM-Signatur. Die Mails werden nun beim Versand signiert.
5. Validierung testen

Nutze Tools wie DKIMCore, MXToolbox oder Google Postmaster Tools, um die Signatur zu prüfen. Alternativ: Sende dir selbst eine Mail an Gmail, öffne den Header und suche nach “Authentication-Results”.

Wichtig: Änderungen im DNS können bis zu 48 Stunden dauern, bis sie weltweit aktiv sind. Sei also nicht nervös, wenn der Test nicht sofort “pass” meldet.

Typische Fehler bei DKIM – und wie du sie vermeidest

DKIM ist mächtig – aber auch sensibel. Ein falsch gesetzter Eintrag, eine fehlerhafte Signatur oder ein vergessener Key-Wechsel führen schnell zu Problemen. Hier die häufigsten Fehlerquellen:

- Falsche Formatierung des TXT-Records: Zeilenumbrüche, fehlende Anführungszeichen oder abgeschnittene Keys sind Klassiker. Immer auf korrekte Syntax achten.
- Zu kurze Schlüssel: Keys mit 1024 Bit gelten als unsicher. Google empfiehlt mindestens 2048 Bit – alles andere wird zunehmend blockiert.
- Fehlende Schlüsselrotation: DKIM-Keys sollten regelmäßig erneuert werden, um Missbrauch zu verhindern. Am besten über zwei Selector parallel arbeiten.
- Mehrere ESPs ohne abgestimmte Selector: Wer mehrere Versanddienste nutzt, braucht pro Dienst einen eigenen Selector – sonst überschreiben sie sich gegenseitig.
- DNS-Caching unterschätzt: Änderungen im DNS brauchen Zeit. Erst testen, wenn sicher ist, dass die Einträge propagiert wurden.

Wer diese Fehler vermeidet, ist der Masse bereits weit voraus – denn gefühlt 80 % aller Domains haben fehlerhafte oder gar keine DKIM-Signatur.

Fazit: Warum DKIM 2025 ein Muss für jedes seriöse E-Mail-Marketing ist

DKIM ist kein nettes Nice-to-have – es ist die Eintrittskarte in den Posteingang deiner Kunden. Ohne DKIM riskierst du nicht nur Zustellprobleme, sondern auch das Vertrauen in deine Marke. In einer Zeit, in der E-Mail-Provider wie Google und Microsoft härter filtern als je zuvor, entscheidet deine technische Setup über Erfolg oder Spam-Friedhof.

Wer heute ernsthaft E-Mail-Marketing betreiben will, kommt an DKIM nicht vorbei – und auch nicht an SPF und DMARC. Together they stand, divided you fall. Also: DNS öffnen, Keys setzen, testen, überwachen. Du willst, dass deine Mails gelesen werden? Dann sorg dafür, dass sie überhaupt ankommen.