# DKIM jenseits von Authentifizierung – Schutz der Markenidentität und -reputation

Gemäß RFC 5863 ermöglicht es die DKIM-Authentifizierung (DomainKeys Identified Mail) einer Organisation, die Verantwortung für die Übertragung einer Nachricht auf eine Weise zu übernehmen, die von einem Empfänger validiert werden kann. Die Organisation kann der Autor, der Ursprungssender oder ein Vermittler sein. Eine E-Mail-Nachricht kann mehrere Signaturen derselben oder verschiedener Organisationen enthalten, die an der Nachricht beteiligt sind.

In diesem Artikel werden die Vorteile von DKIM über den rein technischen Gebrauch hinaus bewertet. Er beinhaltet die Betrachtung weiterer verwandter Standards, die entwickelt wurden, um die E-Mail-Sicherheit zu verbessern und den Erfolg des E-Mail-Marketings zu unterstützen.

## Technische Authentifizierungsmethode

Zusätzlich zu SPF (Sender Policy Framework) ist DKIM eine domänenbasierte Authentifizierung unter Verwendung digitaler Signaturen, bei der die Verschlüsselung mithilfe eines öffentlichen Schlüssels  Domain Name Service (DNS) verwendet wird. Sie überprüft die Integrität der verantwortlichen Organisation für die E-Mail-Nachricht.

DKIM bietet auch einen Mechanismus, mit dem E-Mail-Versender Informationen über ihre E-Mail-Signaturpraktiken veröffentlichen können. Auf diese Weise können E-Mail-Empfänger eingehende Nachrichten effektiver bewerten und verarbeiten.

Diese Authentifizierungsmethode ist für den E-Mail-Empfänger nicht sichtbar, da sie im E-Mail-Header enthalten ist und auf DNS-Ebene ausgeführt wird. Der E-Mail-Empfänger erkennt nur die Absenderadresse im Posteingang. Trotzdem muss die Absenderadresse nicht mit der signierenden DKIM-Domäne übereinstimmen, um die rein technischen Anforderungen per Definition zu erfüllen. Um die technische Integrität einer E-Mail-Nachricht zu bestätigen, wird sie vom E-Mail-Absender signiert, der im Fall von E-Mail-Marketing-Massenmailings in den meisten Fällen ein ESP (Email Service Provider) ist.

## Technisches Kurzdenken über DKIM

Die größte Herausforderung besteht heutzutage darin, gegen subjektive Spam-Klassifizierungen zu kämpfen, die durch Abonnenten-Feedback und Spam-Klicks verursacht werden. Dies schädigt die Absender-Reputation beim Senden von IPs und Domains. Da der Großteil der Einstellungen für das Senden von E-Mails auf gemeinsam genutzten IP-Pools und gemeinsam genutzten DKIM-Domänen basiert, hat die Reputation somit gleichzeitig Einfluss auf mehrere Marken. Aus technischer Sicht entspricht es den RFC-Standards, ermöglicht es jedoch zwielichtigen Marken, sich in dieser Umgebung des ESP zu verstecken und anderen Marken und dem globalen Ruf des ESP zu schaden.

Eine Domain ist eng mit einer Marke verbunden. Dies könnte das Schlüsselelement sein, um eine dedizierte, domänenbasierte Reputation für eine einzelne Marke in einer gemeinsam genutzten ESP-Umgebung aufzubauen. Durch die Verwendung der markenbezogenen Domain in der DKIM-Signatur und -Authentifizierung wird die Verantwortung für den E-Mail-Inhalt teilweise auf die sendende Marke übertragen.

## Domain Alignment und DMARC

Die Authentifizierung der E-Mail-Identität durch DKIM unterstützt auch die globale Kontrolle von "Spam" und "Phishing". Im Jahr 2015 wurde das DMARC-Protokoll (Domain-based Message Authentication, Reporting & Conformance) entwickelt. Es basiert auf SPF und DKIM, um E-Mail-Betrug wie Phishing und Spoofing zu bekämpfen. Die Grundidee besteht darin, die Domain einer Marke zu sichern. Aus diesem Grund ist ein Domin-Alignment von FROM-Domain und der DKIM-Domain wichtig.

Marken können nur geschützt werden, wenn sie transparent hinsichtlich der Domainüberprüfung und der Integrität ihrer eigenen Praktiken und Inhalte sind. Es ist eine logische Konsequenz für Marken, auf ihre eigene Markenidentität und ihren eigenen Ruf zu achten. Dementsprechend müssen ESPs eine dedizierte, markenbezogene DKIM-Authentifizierung einsetzen, um die Reputation für jede einzelne Marke abzugrenzen und die Vermischung der Reputation aufzulösen.

Jeder ESP sollte bereits die Grundlage für die Einführung von DMARC erleichtern, indem er von Anfang an auf Domain-Alignment mit markenbezogenen DKIM-Domains setzt.

## Mehrwert für das E-Mail-Marketing über BIMI

Bis zu diesem Punkt sind DKIM und DMARC ein rein technisches Thema und für E-Mail-Marketer schwer zu verstehen. In vielen Fällen haben E-Mail-Marketer Schwierigkeiten, die weitreichende Bedeutung von E-Mail-Sicherheit zu verstehen. Dies ist der Grund, warum die Einführung von DMARC immer noch ein harter Kampf ist und die DKIM-Authentifizierung nur eine technische „Sache" ist, um die sich der ESP kümmern sollte - in den Augen eines E-Mail-Marketers.

BIMI (Brand Indicators for Message Identification) ist ein guter Weg, um die Lücke zwischen Tech-Nerds und E-Mail-Marketern zu schließen. Der Mehrwert von BIMI ist für E-Mail-Marketer leichter zu verstehen. BIMI schafft immer noch nicht das notwendige technische Verständnis für die Implementierung beim E-Mail-Marketer. Aber die Vorteile von BIMI für den Erfolg ihrer Marke zu nutzen, wird dazu beitragen, die Unterstützung für dedizierte DKIM-Domänen zu erhalten, die notwendig ist um Domain-Alignement zu implementieren und DMARC einzuführen.

## Zusammenfassung und Fazit

Es war eine lange Reise von DKIM zu BIMI. Letztlich sollte BIMI jedoch nicht das einzige Ziel sein. Stattdessen sollte BIMI das Werkzeug sein, um Marken zu erklären, warum es wichtig ist, eine eigene Versand-Domain für ein dediziertes E-Mail-Setup bereitzustellen. DKIM ist das allererste Puzzleteil für die erfolgreiche Implementierung von DMARC und schließlich BIMI. Niemand wird je beginnen, den Berg von oben zu besteigen, aber mit dem Ziel den Gipfel zu erreichen, versteht jeder die Notwendigkeit einer angemessenen Vorbereitung und den richtigen Einstellungen beginnend an der Basis.

ESPs sind die Hauptakteure, die in der Lage sind der sendenden Marke die Vorteile zu erklären und die optimale technische Infrastruktur und Anleitung bereitzustellen.
Sobald gemeinsam genutzte DKIM-Signaturen für ESPs keine Option mehr sind und dedizierte Marken-Domains für die DKIM-Authentifizierung verwendet werden, wird es einfacher DMARC einzuführen, BIMI zu implementieren und gleichzeitig die E-Mail-Sicherheit zu erhöhen und die Vorteile für das E-Mail-Marketing insgesamt zu erhöhen.

Autor: Sebastian Kluth
Technischer Leiter CSA