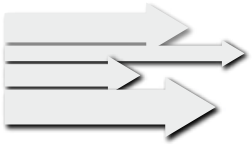
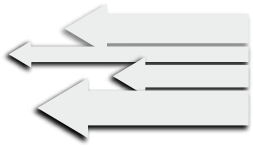
Sichere E-Mail

Was Sie über DKIM wissen sollten

eco Guide zu Domain Keys Identified Mail



DKIM



DomainKeys Identified Mail

DomainKeys Identified Mail (kurz: DKIM) ist ein Verfahren zur Identifikation von E-Mail-Senderdomains.

Das Verfahren bringt, für Endanwender unsichtbar, kurz vor dem Versand kryptografische Signaturen auf E-Mails an. Ein empfangendes System kann prüfen, ob eine Nachricht eine oder mehrere DKIM-Signaturen enthält und prüfen ob die Signaturen intakt sind. Sind die Signaturen intakt, sind damit sowohl Integrität als auch Authentizität der Nachricht bestätigt und die Identität der Senderdomain bestätigt. Ein empfangendes Mailsystem kann, nun da die Identität der Senderdomain bekannt ist, lokal nach einer Reputation der Domain suchen und entsprechend der Reputation die E-Mail annehmen, besonders verarbeiten oder auch ablehnen.

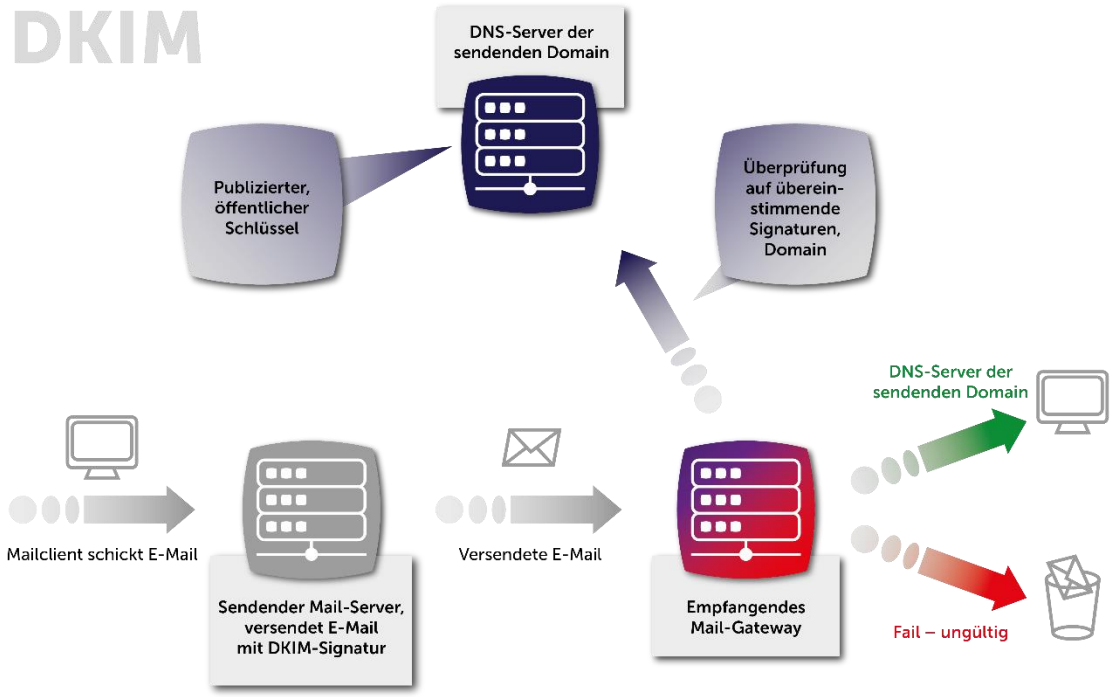
Entstehung

DKIM entstand 2007 aus der Zusammenführung von Yahoos "DomainKeys" und Ciscos "Identified Internet Mail". Es wurde im selben Jahr als RFC 4871 standardisiert, im September 2011 in RFC 6376 aktualisiert und mit den RFCs 8301 sowie 8463 weiter verfeinert.

Wie funktioniert DKIM?

DKIM bringt auf ausgehenden Nachrichten eine Signatur mit zwei Prüfsummen, eine für eine Auswahl an E-Mail-Headern und eine für den E-Mail-Body, an. Das empfangende System kann die Prüfsummen verifizieren, indem es – mit demselben Signaturschlüssel ausgestattet, welchen es aus dem DNS der Senderdomain bezieht – selbst Prüfsummen für E-Mail errechnet und diese anschließend mit den in der E-Mail angegebenen Summen vergleicht. Stimmen die Prüfsummen überein, stammt die Nachricht a) aus der im Enveloppe Sender verwendeten Senderdomain und b) wurde diese seit dem Anbringen der Signaturen nicht modifiziert. DKIM ist also ein Verfahren, um eine Senderdomain zweifelsfrei zu identifizieren und um die Unversehrtheit einer Nachricht nachzuweisen.

DKIM



Der Vorteil von DKIM:

DKIM ist nicht IP-basiert. d. h. jedes beliebige System im Internet kann im Namen einer Senderdomain senden, solange sein kryptografischer Schlüssel nur im DNS der Senderdomain hinterlegt ist. Damit unterliegt es nicht den Einschränkungen des SPF-Mechanismusses und es ist so prinzipbedingt weitaus weniger störanfällig.

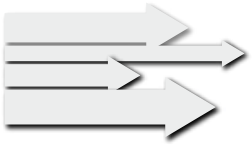
Technische Vorteile gegenüber SPF

Im Gegensatz zu SPF bleibt die DKIM-Signatur auch bei Weiterleitungen gültig, solange der Nachrichteninhalt und die signierten Header unverändert bleiben. Dies macht DKIM besonders wertvoll für Mailinglisten und komplexe E-Mail-Routen.

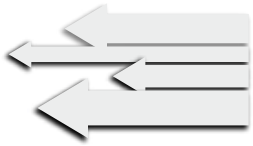
Praktisches Beispiel

Der öffentliche Teil des Schlüssels (Public Key) wird im DNS der signierenden Domain hinterlegt. Dazu ist ein Selektor notwendig.

```
SELECTOR._domainkey.DOMAIN.TLD TXT "v=DKIM1; k=rsa; p=PUBLIC_KEY"
```



DKIM



Es ist möglich, in einer Domain mehrere DKIM Keys - mittels unterschiedlichen Selektoren - zu setzen. Empfohlen wird auch, Keys und Selektoren regelmäßig zu rotieren und - für größere Organisationen - unterschiedliche Key/Selektor Paare für unterschiedliche Einsatzzwecke zu verwenden.

Auf https://dkim.org/ finden Sie weitere Details zur Implementierung von DKIM

Weitere Informationen bezüglich des Zusammenspiels von DMARC, DKIM und SPF finden Sie in den Dokumenten der KG E-Mail in unserem Downloadbereich.

Weitere Informationen bezüglich des Zusammenspiels von DMARC, DKIM und SPF finden Sie in den Dokumenten der Kompetenzgruppe-E-Mail in unserem Downloadbereich auf https://www.eco.de

Kontakt:
Michael Weirich
Projekt Manager IT-Sicherheit
eco – Verband der Internetwirtschaft e. V.

Mobil: +49(0)171 – 554 0303
E-Mail: michael.weirich@eco.de
Web: https://www.eco.de/