DKIM

Inhaltsverzeichnis

DKIM signiert E-Mails kryptografisch, damit empfangende Mailserver prüfen können, ob eine Nachricht unverändert ist und zur angegebenen Domain passt.

DomainKeys Identified Mail, kurz DKIM, ist ein Verfahren zur E-Mail-Authentifizierung. Ausgehende Nachrichten werden mit einem privaten Schlüssel signiert, der öffentliche Schlüssel liegt als DNS-Record vor.

1 Funktionsweise

Der sendende Mailserver fügt der Nachricht eine DKIM-Signatur hinzu. Empfänger prüfen diese Signatur über den öffentlichen Schlüssel im DNS.

- **Selector:** benennt den verwendeten Schlüssel.
- **DNS-TXT-Record:** enthält den öffentlichen Schlüssel.
- **Signatur:** schützt ausgewählte Header und Inhalte vor Veränderung.

2 Zusammenspiel mit SPF und DMARC

DKIM ist besonders wirksam, wenn es mit SPF und DMARC kombiniert wird.

- SPF prüft erlaubte sendende Server.
- DKIM prüft Signatur und Integrität.
- DMARC legt fest, wie Fehler behandelt werden.

3 Betriebshinweise

DKIM-Schlüssel sollten sicher verwaltet und bei Bedarf rotiert werden.

- Private Schlüssel nicht öffentlich ablegen.
- Mehrere Selektoren für Rotation nutzen.
- Signaturen nach Mail-Gateways und Weiterleitungen prüfen.

4 Fazit

DKIM ist ein wichtiger Baustein moderner E-Mail-Sicherheit und verbessert die Vertrauenswürdigkeit ausgehender Nachrichten.