DKIM

Es gibt mehrere Verfahren um die Echtheit von E-Mails zu überprüfen und Absende-Adressen gegenüber SPAM Missbrauch zu schützen.

DKIM - DomainKeys Identified Mail

Was ist das DKIM-Protokoll?
Dieses Protokoll ist eine Methode der E-Mail-Authentifizierung. Es ermöglicht die Signatur Ihrer E-Mail mit Ihren Domainnamen, wie bei einem Brief, den Sie mit Ihrer Unterschrift versehen. Der Empfänger Ihrer E-Mail hat die Sicherheit, dass die erhaltene E-Mail von Ihnen stammt und während der Übertragung nicht geändert wurde. Das Verwenden eines DomainKeys dient dazu, das Fälschen des Absenders einer E-Mail zu erschweren.

Auch die Header werden gegen Manipulationen gesichert. Das Protokoll soll möglichst flexibel einsetzbar sein, auch in mehrstufigen Mail-Systemen und bei E-Mail-Dienstleistern. Daher sind einige Zusatzinformationen erforderlich. Der Server fügt in die E-Mail einen zusätzlichen Header "DKIM-Signature" ein, an dem sich die Probleme und Prinzipien des Verfahrens zeigen. Er sieht beispielsweise so aus:

```
DKIM-Signature: v=DKIM1;
 a=rsa-sha1; c=relaxed
/simple;
d=example.at;
s=mail111222; i=dau@sub.
example.at;
h=Date:From:To:Subject:
Message-ID:References:
Content-
Type:Content-
Disposition:Content-
Transfer-Encoding;
bh=8FBe8u6BvmKcvYyKlx+oY
vPBSj=; b=I+oWYOxFAk
```

DKIM erstellen und prüfen

Um einen DKIM Eintrag zu erstellen, können Sie als Beispiel einen der vielen Generatoren verwenden, die Online zur Verfügung stehen. Zum Überprüfen kann man auch auf diverse Web-Tools zurückgreifen, wie beispielsweise: https://protodave.com/tools/dkim-key-checker/

Info

Der Schlüssel lässt sich auch auf der Kommandozeile mit dem Befehl `nslookup` oder `dig` abfragen.

Mit dem Befehl:

```
nslookup -type=TXT mail111222._domainkey.example.net
```

lässt sich der Schlüssel abfragen, wenn Sie über einen shell-Zugriff verfügen. Der zurückgelieferte Wert sieht bei Erfolg ungefähr so aus:

```
...
v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC0N
...
```

Die Felder enthalten die DKIM-Version (**v=**, optional), den Schlüsseltyp (**k=**, optional) und den Schlüssel selbst (**p=**).
Durch unterschiedliche Selektoren kann eine Domain mehrere Schlüssel benutzen. Der RFC empfiehlt, den Schlüssel
regelmäßig zu wechseln und den alten als ungültig zu kennzeichnen. Dazu lässt der Admin den **TXT-Record** in seinem
DNS, löscht jedoch den eigentlichen Schlüssel, also den Teil hinter p=. Über eine Versionsnummer oder Datumsangabe
im Selektor lässt sich dann leicht zwischen gültigen und widerrufenen Schlüsseln umschalten. Die Signatur umfasst
den Körper der Mail und die Header, um beispielsweise sicherzustellen, dass sich kein Fälscher als Absender ins
From: einträgt. Damit unterwegs eingefügte oder unwichtige Header die Signatur nicht stören, enthält der DKIM-Header
eine Liste der signierten Felder (**h=**). Hier können auch Header stehen, die in der E-Mail gar nicht vorkamen, um zu
verhindern, dass sie unterwegs eingefügt werden. Das Feld **i=** enthält die "Identity", für die signiert wurde. Das kann
der komplette Absender sein oder auch die (Sub-)Domain, für die der signierende Server zuständig ist. Das Beispiel zeigt,
dass die E-Mail-Adresse durchaus zu einer Subdomain der mit d= angegebenen Domain gehören darf. Im Header steht der Hash
des Body (**bh=**), damit der Empfänger Veränderungen auch dann bemerken kann, wenn der öffentliche Schlüssel durch eine
DNS-Störung nicht verfügbar ist oder widerrufen wurde. Am Ende steht dann mit **b=** die eigentliche Signatur.