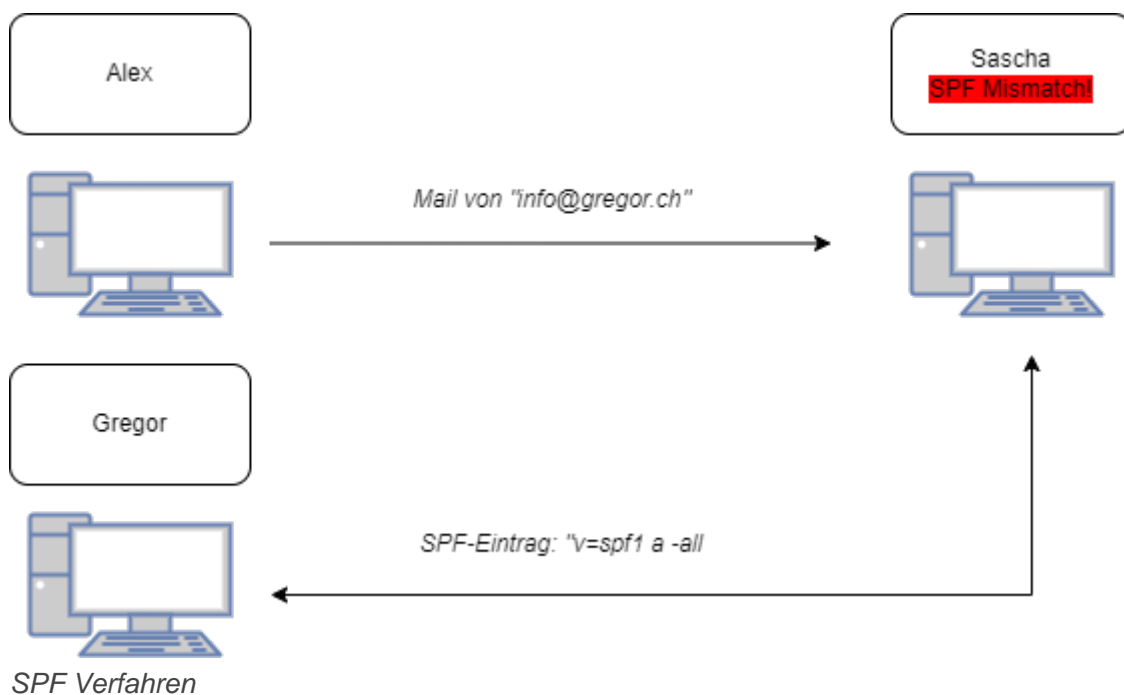
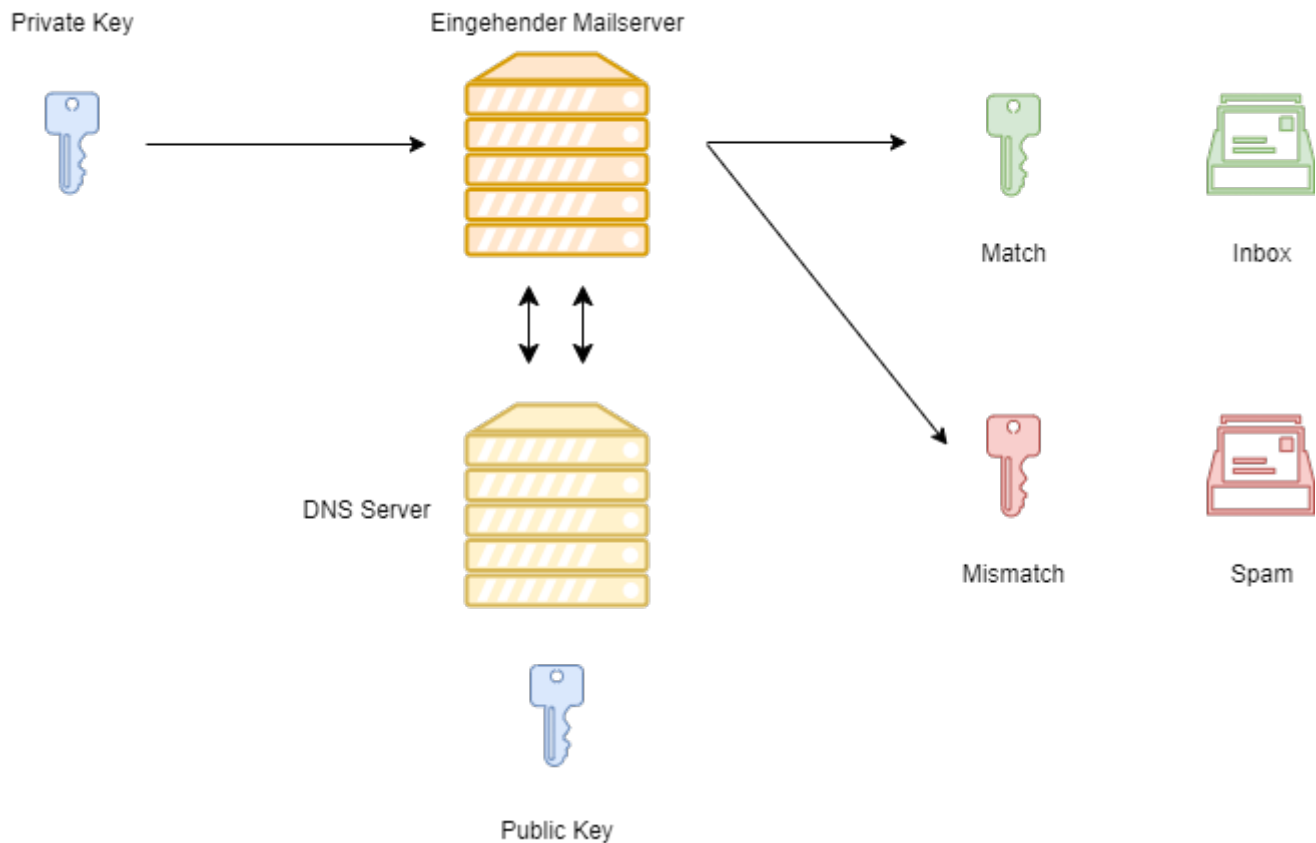


# Abwehr vor Spam

SPF (Sender Policy Framework)	Der SPF Eintrag soll das Versenden von gefälschten und nicht vertrauenswürdigen Absendern verhindern. Dieses Verfahren dient somit der Spam-Abwehr. Der SPF wird in der DNS-Zone festgelegt.
DKIM (Domain Key Identified Mail)	DKIM ist ein Protokoll, das eine Nachricht verifiziert, um vor unerwünschtem Spam und Pishing-Mails zu schützen. Es gibt einen Public und einen Private Key. Der Private Key befindet sich beim Benutzer und sendet Nachrichten Verschlüsselt. Der Public Key befindet sich in der DNS-Zone.
DMARC (Domain-based Message Authentication, Reporting and Conformance)	DMARC baut auf dem selben System auf wie SPF und DKIM. Der unterschied besteht darin, das dem DMARC Funktionen zugewiesen werden können, wie bei Situation gehandelt werden soll. z. .B können so Berichte wie LOGS an den Empfänger geschickt werden.





*DKIM Verfahren*

*DMARC Verfahren*

## Greylisting

Beim Greylisting handelt es sich um ein Verfahren zur Abwehr vor Spam und weist E-Mails zunächst ab. Nach der Abweisung wird eine Sperre von meistens 90 Sekunden verhängt bevor man eine neue E-Mail schicken kann.

## Blacklisting

Beim Blacklisting werden bestimmte Absender und Ausdrücke permanent gesperrt. Es gibt viele Anbieter, die Listen zur Verfügung stellen, in denen Bekannte Absender und Ausdrücke schon erfasst sind.

Man kann aber auch eine eigene Blacklist über verschiedene Mailprogramme erstellen.

## Aufbau des DKIM Eintrags

Name	Typ	Inhalt
[ selector ]. _domainkey. [ domain ]	TXT	v=DKIM1; p=76E629F05F709EF665853333EEC3F5ADE69A 2362BECE40

Der DKIM Eintrag in der DNS Zone definiert den Public Key.

## DKIM Header

Beispiel für einen DKIM-Header:

```
v=1; a=rsa-sha256; d=example.com; s=big-email; h=from: to: subject;  
bh=uMixy0BsCqhbru4fqPZQdeZY5Pq865sNAn0AxNgUS0s=;  
b=LiIvJeRyqMo0gngiCygwpiKphJjYezb5kXBKCNj8DqRVcCk7obK60Ug4o+EufEbB  
tRYQfQhgIkx5m70IqA6dP+DBZUcsJyS9C+vm2xRK7qyHi2hUFpYS5pkeiNVoQk/Wk4w  
ZG4tu/g+0A49mS7VX+64FXr79MPwOMRRmJ3lNwJU=
```

Eintrag	Beschreibung
v=1	Version des DKIM
d=example.com	Domainname des Absenders
s=big-email	Selector des Absenders
h=from: to: subject	Auflistung der Header-Felder die zur Erstellung der digitalen Signatur benötigt werden.
bh=uMixy0BsCqhbru4fqPZQdeZY5Pq865sNAn0AxNgUS0s=;	Hash des E-Mail Text. Dies ist eine Mathematische Funktion, die für die Berechnung der digitalen Signatur für den Empfangenden Mail-Server
b=LiIvJeRyqMo0gngiCygwpiKphJjYezb5kXBKCNj8DqRVcCk7obK60Ug4o+EufEbB tRYQfQhgIkx5m70IqA6dP+DBZUcsJyS9C+vm2xRK7qyHi2hUFpYS5pkeiNVoQk/Wk4w ZG4tu/g+0A49mS7VX+64FXr79MPwOMRRmJ3lNwJU=	Digitale Signatur, die aus h und bh erzeugt und mit dem privaten Schlüssel signiert wurde.

## Nützliche Links:

[SPF](#)

[DKIM](#)

[DMARC](#)

---

Revision #18

Created 12 July 2023 16:30:54 by Alexander Greub

Updated 15 August 2023 13:39:20 by Alexander Greub