

# E-Mail und Spam-Abwehr - SPF, DKIM und DMARC



# Zustellbarkeit von E-Mails

## Methoden zur Authentifizierung von E-Mail-Absendern ergänzt

01.02.2024

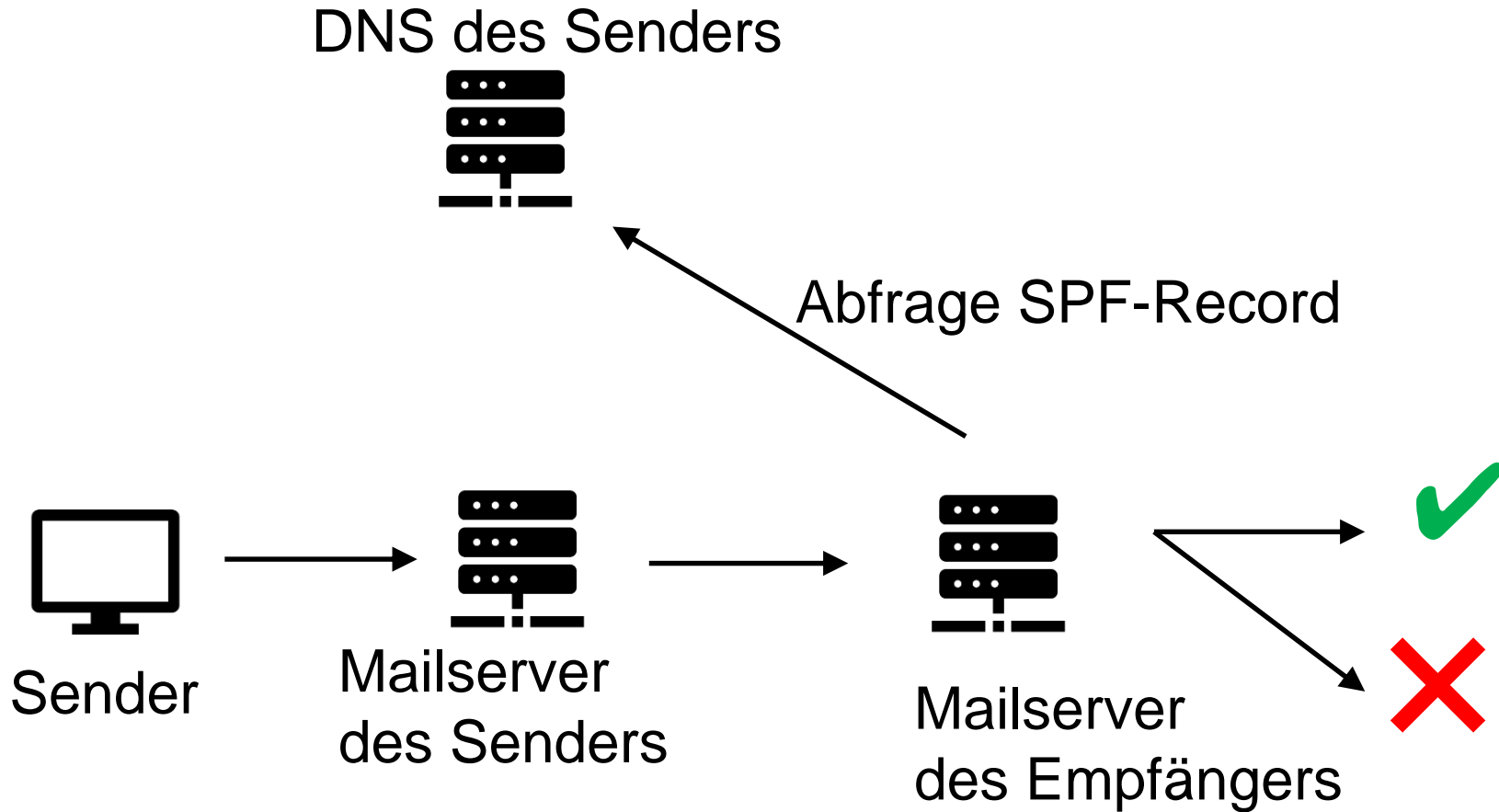
*Diese Newsmeldung richtet sich in erster Linie an die IT-Beauftragten und Administratoren der Institute. Als normaler Nutzer des Mailsdienstes müssen Sie nichts weiter unternehmen.*

→ Google, Microsoft und Gmx/Web nehmen keine Mails mehr ohne SPF/DKIM/DMARC an

# Grundlegendes

- SPF, DKIM, DMARC
  - Möglichkeit auf Empfängerseite gefälschte Mails zu erkennen
  - Die Senderseite muss die Verfahren einrichten/unterstützen
- SPF unterstützen wir seit einigen Jahren
- DKIM/DMARC ist seit Jahresanfang flächendeckend eingerichtet
- Voraussetzung um größere Mengen Mails zu versenden

# SPF – Sender Policy Framework - Ablauf



## Beispiel: luis.uni-hannover.de

TXT-Record für luis.uni-hannover.de in unserem DNS:

**v=spf1 [...] ip4:130.75.2.114 [...] ~all**

Header einer Mail an Google:

**Received: from mailgate2.uni-hannover.de [130.75.2.114]  
by mx.google.com**

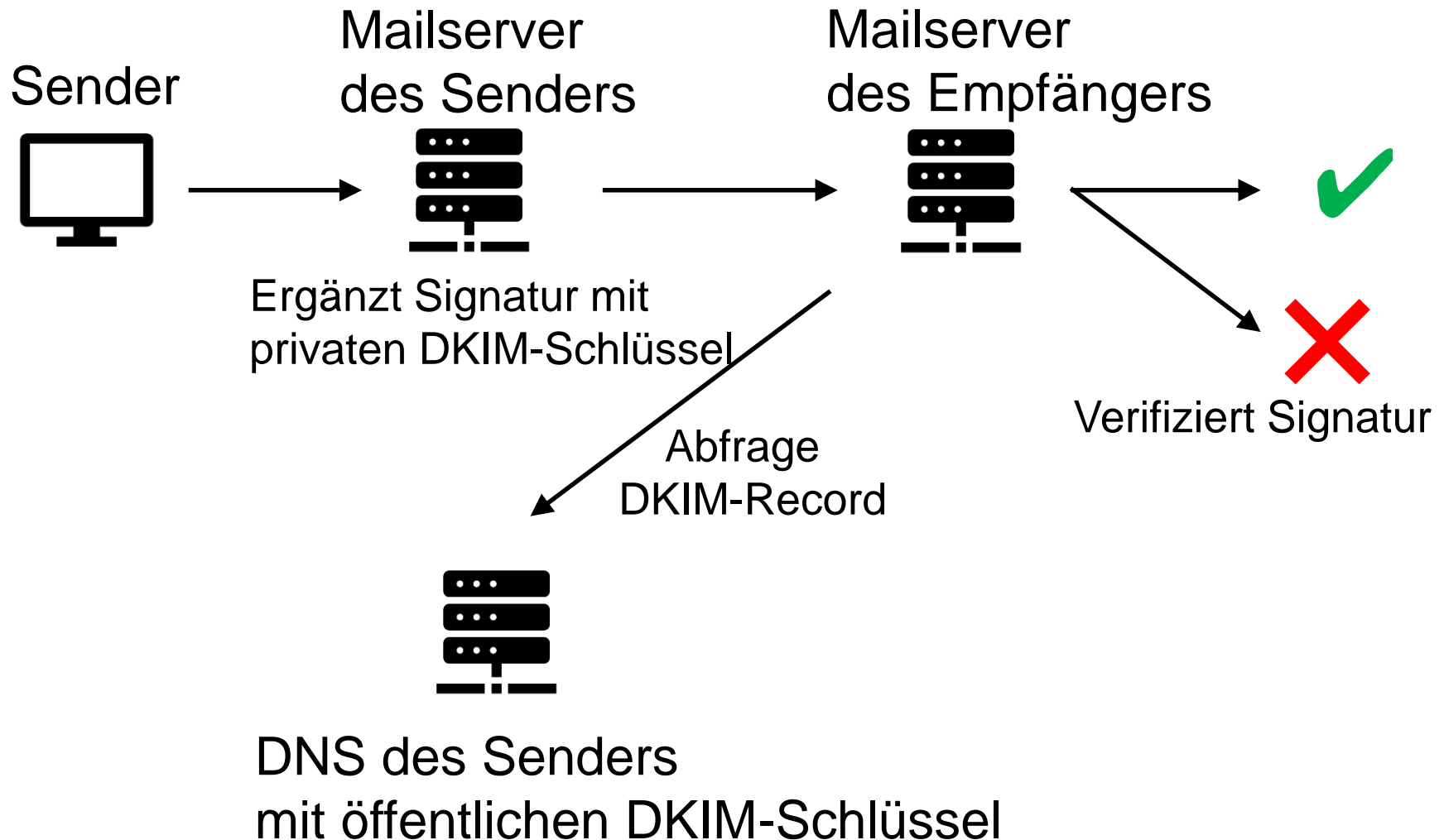
**[...]**

**Return-Path: <moehrle@luis.uni-hannover.de>**

**Received-SPF: pass**

**(google.com: domain of moehrle@luis.uni-hannover.de designates  
130.75.2.114 as permitted sender) client-ip=130.75.2.114;**

# DKIM - DomainKeys Identified Mail - Ablauf



# DMARC - Domain-based Message Authentication, Reporting and Conformance

- Angabe, wie mit fehlerhaften Mails umgegangen wird
- Nur wenn SPF und DKIM ungültig/nicht vorhanden
- Weiterer DNS-Eintrag für die Policy:
  - **None**
  - Quarantine
  - Reject

# Beispiel: Mail an externen Anbieter

Header einer Mail an Google:

**Authentication-Results: mx.google.com;**

**dkim=pass header.i=@uni-hannover.de  
header.s=2024all [...];**

**spf=pass (google.com: domain of moehrle@luis.uni-  
hannover.de designates 130.75.2.114 as permitted sender)  
smtp.mailfrom=moehrle@luis.uni-hannover.de;**

**dmARC=pass (p=NONE sp=NONE dis=NONE) header.from=uni-  
hannover.de**



# Probleme

- Keine allgemeine Lösung gegen SPAM
  - Auch Spammails können SPF/DKIM/DMARC erfüllen
  - Gehackte Mailboxen erfüllen dies ebenfalls
- Um/Weiterleitungen an externe Anbieter sind problematisch
  - Absender passt nicht zum SPF-Record
  - DKIM u.U auch ungültig

-> Mails werden zum Teil abgewiesen

# DFN – SPAM-Abwehr

- Auswertung SPF/DKIM/DMARC erfolgt durch den DFN
  - Einfluss auf den SPAM-Score
- Weitere Maßnahme seit letztem Jahr:
  - Mails die von außerhalb der Uni kommen und eine unsere Maildomains als Absender haben, erhalten einen hohen SPAM-Score

# Aktueller Hinweis – Dell

- Abfluss von Kundendaten bei Dell
  - Name
  - Anschrift
  - Daten zum Bestellvorgang (inkl. Service-Tags)
- Erhöhte Aufmerksamkeit bei Mails von Dell und Mails die ähnlich aussehen
- Sowie ungefragtem Telefonsupport

# Vielen Dank für Ihre Aufmerksamkeit

