



DFN-Listserv

Der Dienst und die Technik dahinter

Olaf Hopp, Sabine Lorenz, KIT, 7.10.2025

1. Überblick DFN-Listerv
2. Komponenten des Informationsverbundes
3. Sympa-Funktionen zum Einbinden von Abonnenten und Empfehlungen zur Konfiguration von Listen

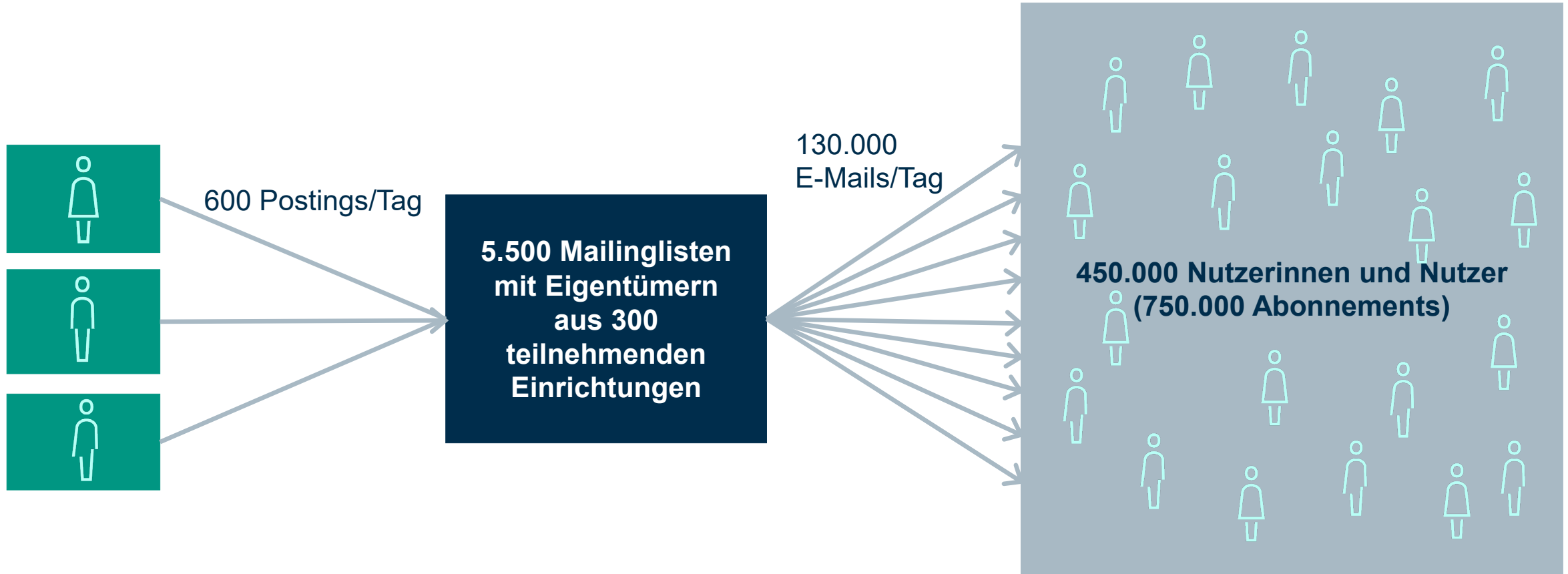
Was ist der Dienst DFN-Listserv?

Plattform für Mailinglisten für DFN-Mitglieder*

- **Hosting:**
auf Systemen des KIT (Karlsruher Institut für Technologie)
- **Verwaltung der Listen:**
durch Listeneigentümer in den jeweiligen Einrichtungen
- **URL der Dienstwebseite:**
<https://www.listserv.dfn.de>
- **Domain und E-Mail-Adressen der Mailinglisten:**
E-Mail-Adressen aller Mailinglisten haben das Format `<Listenname>@listserv.dfn.de`
- **Support und Betrieb:**
listmaster@listserv.dfn.de am KIT → 2nd-Level Support + Ansprechpartner

* Voraussetzung: DFN-Internet oder DFN-Dienst-Paket

Statistikdaten DFN-Listserv



Mailinglistenserver

Betriebssystem

- Debian GNU/Linux

Verwendete Software

- Mailinglisten-Software Sympa
- MTA Exim
- Webserver Apache
- Datenbank MariaDB



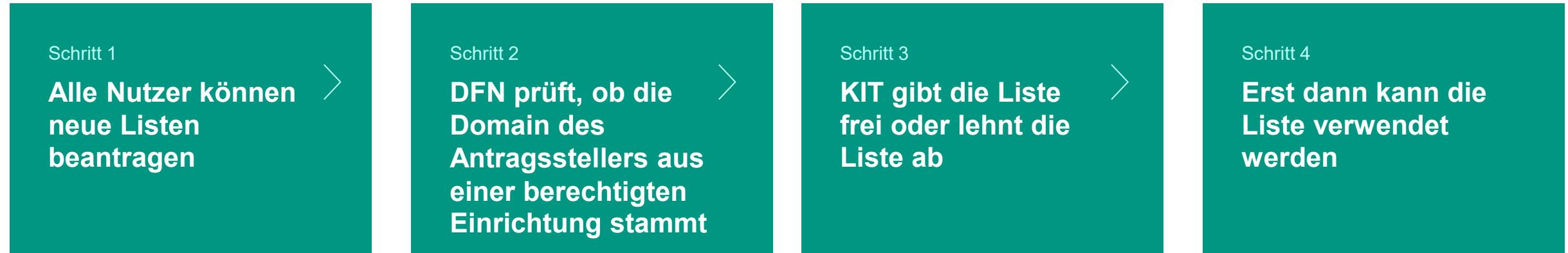
Neuerungen bei DFN-Listserv

- **Dienstvereinbarung mit dem DFN**
inklusive AVV und TOMs*
- **Zuordnung der Listen zu den Einrichtungen**
→ Listen werden über einen Parameter den Einrichtungen zugeordnet
- **Sichtbare Zuordnung durch Präfix**
→ Listennamen sollten das Kürzel der Einrichtung als Präfix tragen
- **Dezentraler Support**
→ First-Level-Support erfolgt durch die teilnehmenden Einrichtungen selbst

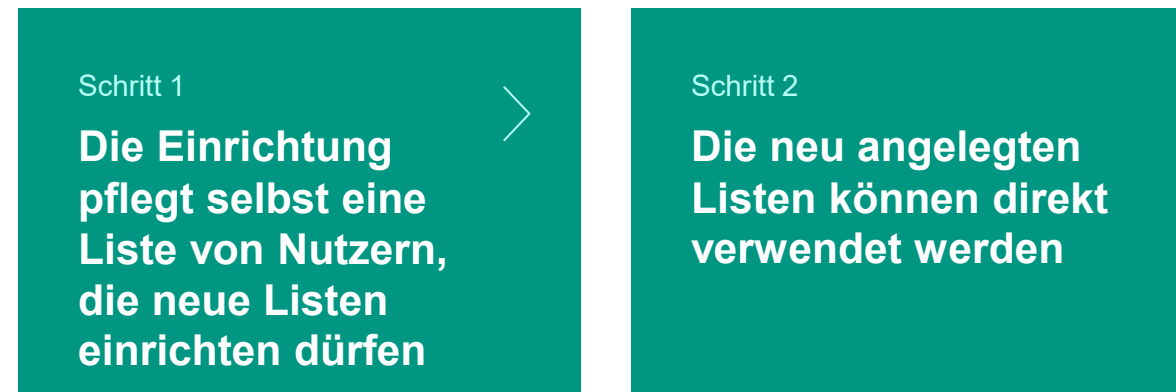
*AVV = Auftragsverarbeitungsvertrag, TOMs = Technisch Organisatorische Maßnahmen

Neuer Prozess zum Anlegen von neuen Listen

Bisher:

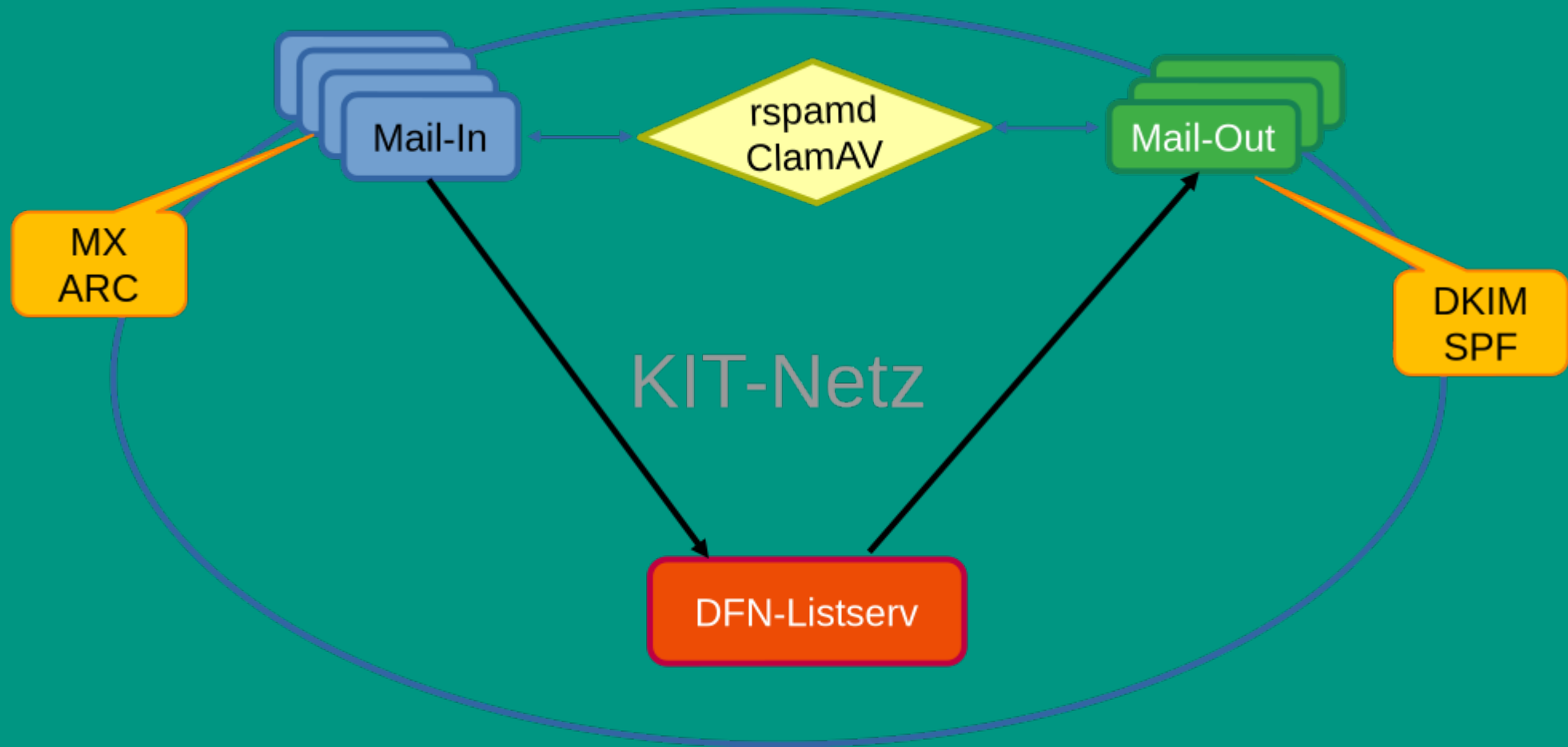


Neu:



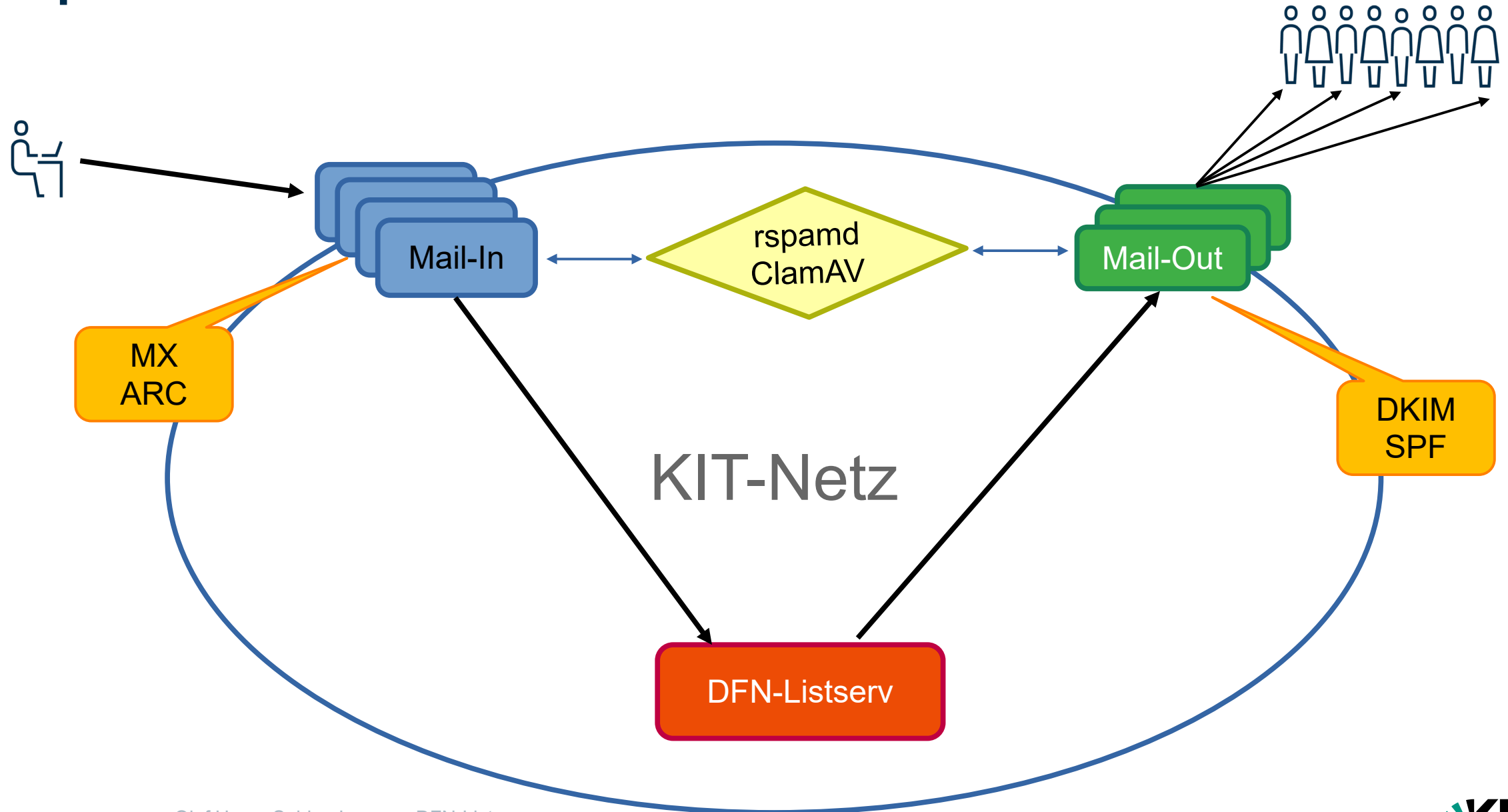
Vorteile:

- Die Listen können sofort verwendet und an die zukünftigen Eigentümer weitergegeben werden
- Kontrolle über die Einrichtung von neuen Listen liegt bei den Einrichtungen selbst



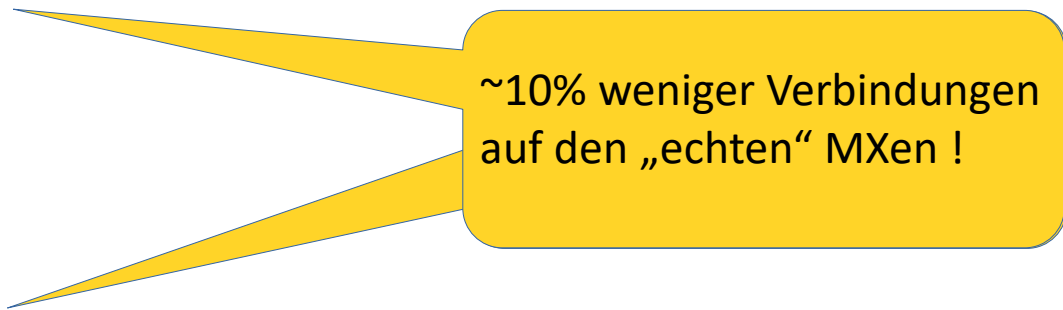
Komponenten des Informationsverbundes

Komponenten des Informationsverbundes



MX-Records

- **# dig listserv.dfn.de mx +short**
- 5 scc-spamtrap-no-smtp-here.scc.kit.edu.
- 10 mx01.kit.edu.
- 10 mx02.kit.edu.
- 10 mx03.kit.edu.
- 10 mx04.kit.edu.
- 100 scc-spamtrap-always-defer.scc.kit.edu.



~10% weniger Verbindungen
auf den „echten“ MXen !

SPF – Sender Policy Framework

- Bei SPF hinterlegt man in einem DNS Text-Record, welche IPs berechtigt sind, eine bestimmte Domain im Envelope-From zu verwenden
- Ferner trifft man eine Aussage, was bei Verstößen gemacht werden soll
- Mails vom DFN-Listenserver haben immer `<listenname>-owner@listserv.dfn.de` als Absender im Envelope
- ```
dig listserv.dfn.de txt | grep spf
listserv.dfn.de. 441 IN TXT "v=spf1 include:spf.scc.kit.edu ~all"
```
- „~all“ (=Softfail), denn sonst gehen Weiterleitungen kaputt !

# DKIM – DomainKeys Identified Mails

- DKIM signiert wesentliche Teile der Mailheader und den Body mit einem kryptografischen Hash
- Empfangende entfernte Mailserver können den Public Key des Signing Keys im DNS abfragen und die Signatur überprüfen
- Entscheidend ist hier die Domain des Header-From
- DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; **d=listserv.dfn.de;**  
**s=kit1;** h=List-Archive:List-Owner:[...];  
bh=LRPsBkqlckhMu9xxRbHV4vDCmrBVTrEdU/q/BVhhkjc=; b=NxfbOPY4hy8uE8GPSPzEnjyX4o[...]
- # dig kit1.\_domainkey.listserv.dfn.de | grep ^kit1  
**kit1.\_domainkey.listserv.dfn.de. 892 IN CNAME kit1.\_domainkey.kit.edu.**
- # dig kit1.\_domainkey.kit.edu TXT +short  
**"v=DKIM1; k=rsa; p=MIIBIjA[...]"**
- Setzt man bei der DFN-Liste „*DMARC-Protect = all*“ wird der Header-From umgeschrieben zu  
**From: "Olaf Hopp" (via testliste Mailing List) <[testliste@listserv.dfn.de](mailto:testliste@listserv.dfn.de)>**
  - → erzeugt neue (gültige) DKIM Signatur von „**listserv.dfn.de**“

# DMARC

## Domain-based Message Authentication, Reporting and Conformance

- Wir haben SPF und machen DKIM
- Mit DMARC sagen wir dem Empfänger, was bei Verletzung von SPF und/oder DKIM gemacht werden soll:
  - „none“, „quarantine“, „reject“
  - Informiere uns wie angegeben über Verletzungen
- ```
# dig _dmarc.listserv.dfn.de TXT
_dmarc.listserv.dfn.de. [...] CNAME _dmarc.kit.scc.edu.
_dmarc.scc.kit.edu. [...] v=DMARC1; p=none; adkim=r; aspf=r; rua=mailto:dmarc@scc.kit.edu
```

 - Policy = „none“
 - Abgleichmodus SPF u. DKIM = „relaxed“
 - Aggregiert Reports an das KIT-CERT

ARC – Authenticated Received Chain

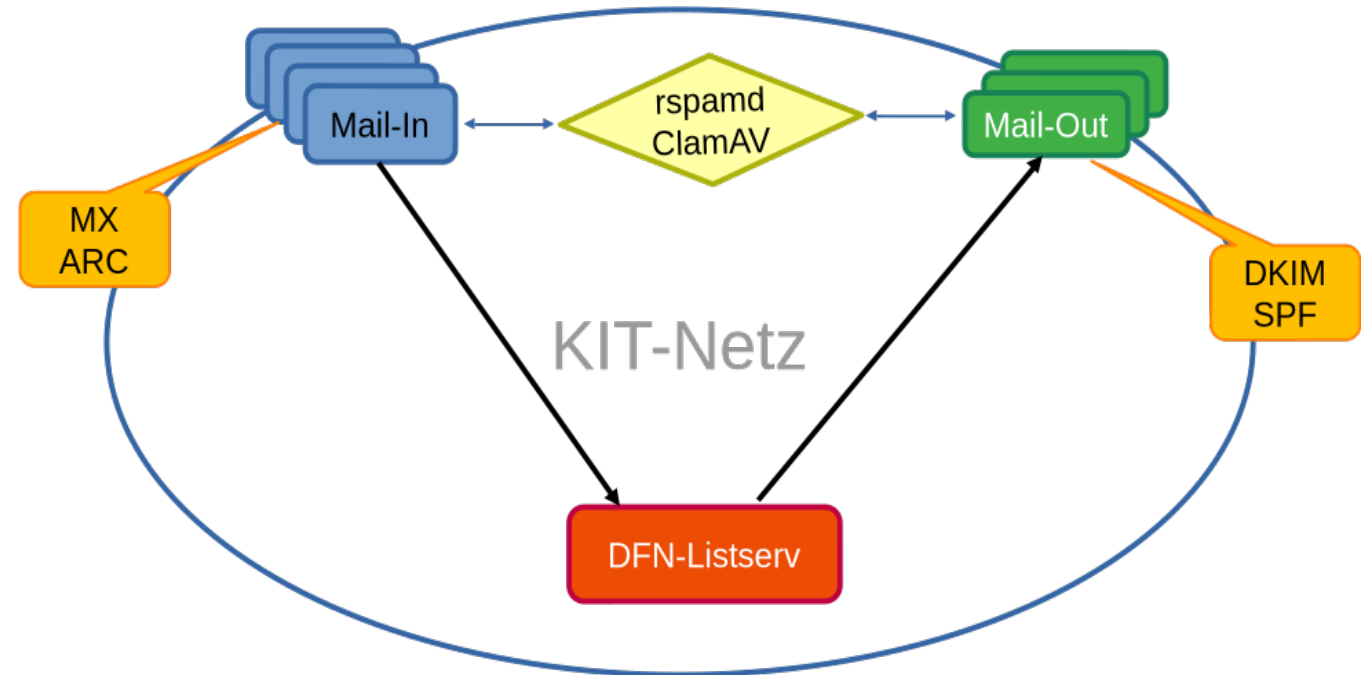
- Findet auf den Maileingangsservern statt
- Ich weiß, dass die Mail potentiell hinter mir (auf dem Listenserver) gleich kaputt gemacht wird
- Bis hier stimmen DKIM und/oder SPF
- Ich stemple dies bis hierhin schon mal ab → crypto hash
- „*vertraut mir, bis hierhin ist alles OK*“
- **Authentication-Results:** mx04.kit.edu; **dkim=pass** header.d=example.com header.s=2017 header.b=T8qqzkEq; **spf=pass** (mx04.kit.edu: domain of foo.bar@example.com designates 127.0.0.1 as permitted sender) smtp.mailfrom=foo.bar@example.com; **dmARC=pass** (policy=none) header.from=example.com
- **ARC-Message-Signature:** i=1; a=rsa-sha256; c=relaxed/relaxed; **d=kit.edu; s=kit1;** t=1754911865; h=from:sender:reply-to:[...]; bh=47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=; b=jo5VT9RGrNis[...]
- **ARC-Seal:** i=1; **s=kit1; d=kit.edu;** t=1754911865; a=rsa-sha256; cv=none; b=jonK6clQc6R9MHyztqTqZuXQA+Q2e5RUrDqxACf[...]

rspamd + ClamAV

- Malware- und Spamscan findet sowohl eingehend als auch ausgehend statt
- „früher“ Spamassassin
- Vor 4 Jahren Umstieg auf rspamd
 - deutlich geringere Systemlast
 - Gemeinsame Redis-DB für alle Systeme
 - Viele selbstgeschriebene eigene Regeln
- Dazu Heuristik zum Schutz vor ausgehendem Spam
 - Bounces pro Absender und Zeitfenster
 - Spampunkte pro Absender und Zeitfenster
 - Reply-To: != From: ?
 - [...]
 - Sperrt Absenderadresse, legt Mails in Quarantäne, erzeugt Ticket
 - **nicht** für DFN-Listenmails :-)

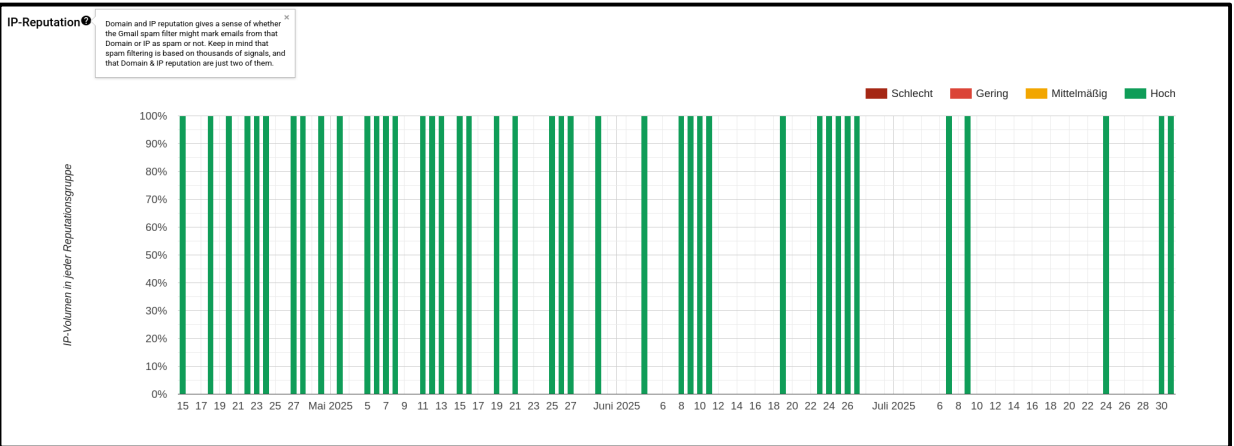
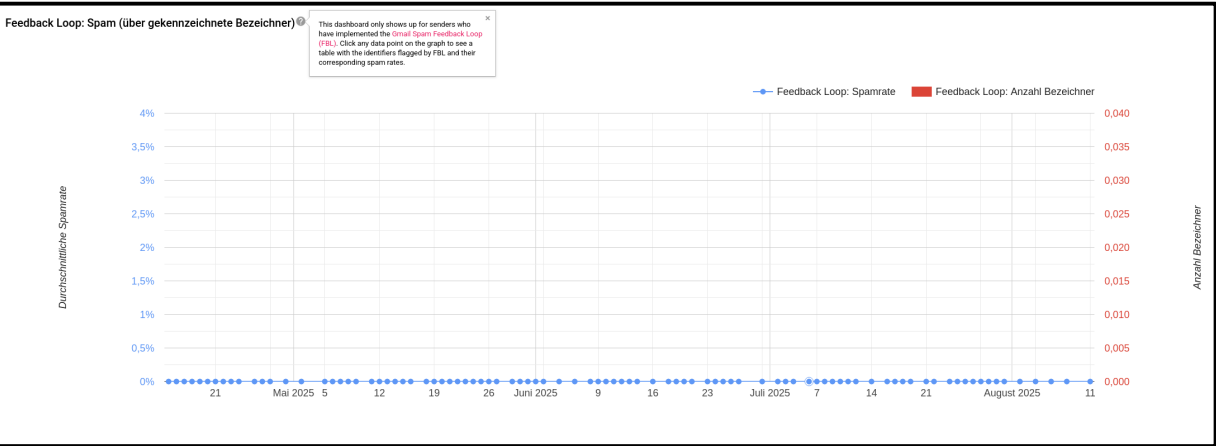
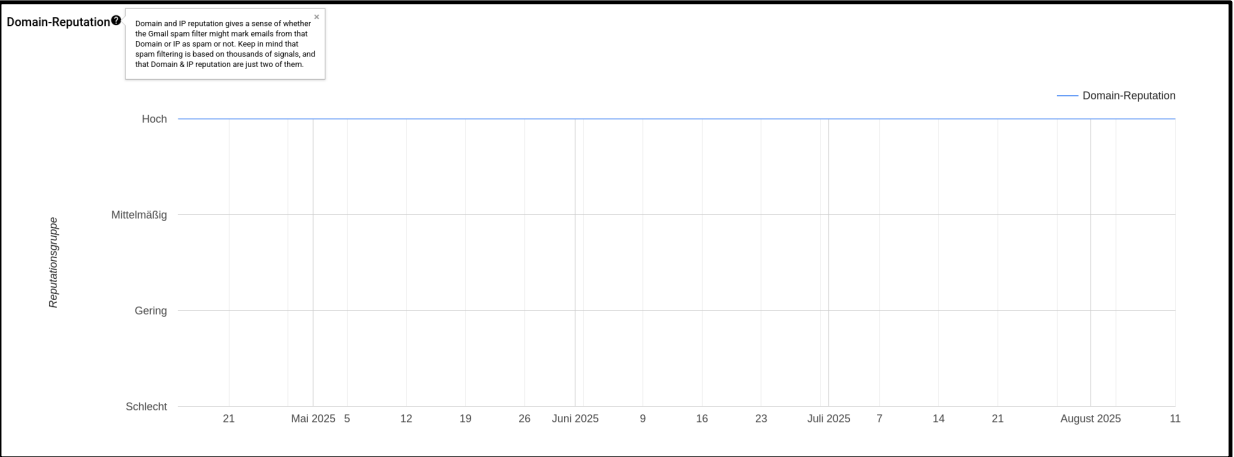
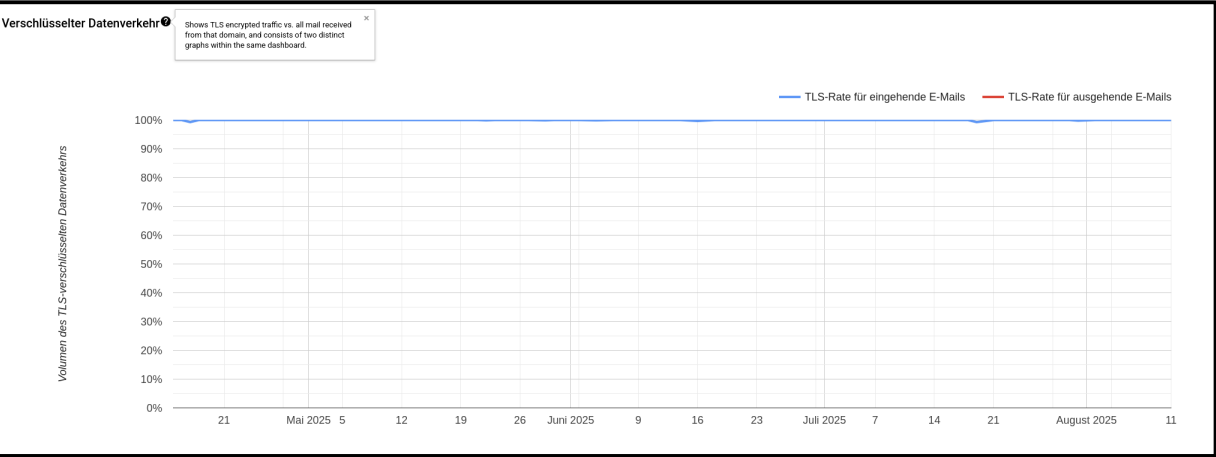
Komponenten Mailserver

- MX
- SPF
- DKIM
- DMARC
- ARC
- rspamd + ClamAV
- *DANE (setzt DNSSEC voraus → NA)*
DNS-based Authentication of Named Entities

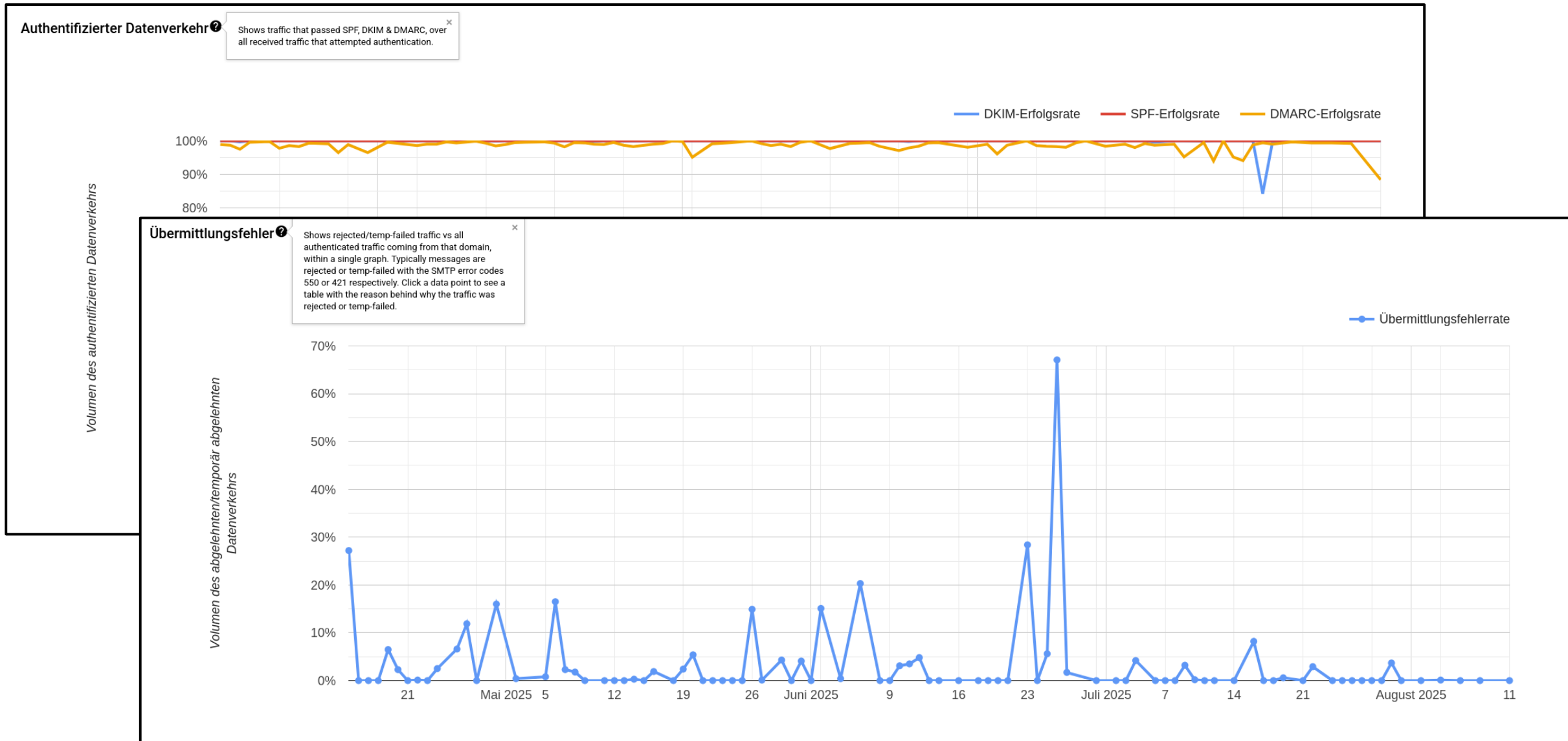


- *Siehe auch*
Dr. P. Wullinger „SPooFING: Verfahren zur Absenderprüfung bei E-Mail“, 82. DFN-Betriebstagung 26.3.25
https://www.dfn.de/wp-content/uploads/2024/10/Forum_Mail_Wullinger-Mail-AK-SPFoofing.pdf

Google Postmastertools



Google Postmastertools





Sympa-Funktionen zum Einbinden von Abonnenten und Empfehlungen zur Konfiguration von Mailinglisten

Schachtelung von Listen

Einbindung von Abonnenten aus anderen Listen mit zyklischer Synchronisation

Vorteile:

- Abonnenten erhalten die Berechtigungen der Liste
- Keine Loops

Bitte keine Mailinglistenadressen als Abonnenten!

Hinweis:

- Aus Datenschutzgründen kann diese Eintragung nur von den Listmastern durchgeführt werden

Webseite mit den Datenquellen

Listeneinbindung ?

Kurzname für diese Quelle
include_list kindliste_1

Name der zu inkludierenden Liste
kindliste_1

Kurzname für diese Quelle
include_list kindliste_2

Name der zu inkludierenden Liste
kindliste_2

Abonnenten-Tabelle

Listenabonnenten								
☒	E-Mail	Domäne	Bild	Name	Empfang	Quellen	Datum	Letzte Aktualisierung
☐	olaf.hopp@kit.edu				standard (direkter Empfang)	include_list kindliste_2	23 Jul 2025	23 Jul 2025
☐	s.lorenz@kit.edu				standard (direkter Empfang)	include_list kindliste_1	23 Jul 2025	23 Jul 2025
☐	sabine.lorenz@kit.edu				standard (direkter Empfang)	include_list kindliste_1	23 Jul 2025	23 Jul 2025

Einbindung aus externen Quellen

Einbindung von Abonnenten aus externen Quellen mit zyklischer Synchronisation

- **Datei-Import über URL**
→ E-Mail-Adressen werden automatisch eingebunden
- **LDAP-Abfrage**
→ Direkte Integration aus dem Verzeichnisdienst

Vorteile:

- Keine manuelle Pflege der E-Mail-Adressen nötig
- Eigentümer können die Eintragungen selbständig vornehmen

Webseite mit den Datenquellen

Einbindung entfernter Dateien ☐ Löschen

Kurzname für diese Quelle

test_include_url

URL der Daten

https://www.test2.lists.kit.edu/test.txt

Benutzer auf entferntem Rechner

user1@example.com

Passwörter verwalten

Passwort auf entferntem Rechner

•••••

Abonnenten-Tabelle

Listenabonnenten								
☑	E-Mail	Domäne	Bild	Name	Empfang	Quellen	Datum	Letzte Aktualisierung
☐	olaf.hopp@kit.edu				standard (direkter Empfang)	abonnieren	04 Aug 2025	04 Aug 2025
☐	s.lorenz@kit.edu				standard (direkter Empfang)	test_include_url	12 Aug 2025	12 Aug 2025
☐	sabine.lorenz@kit.edu				standard (direkter Empfang)	test_include_url	04 Aug 2025	04 Aug 2025

Empfehlungen zur Konfiguration von Mailinglisten

Aktivierung des DMARC-Protection-Modus für alle E-Mails

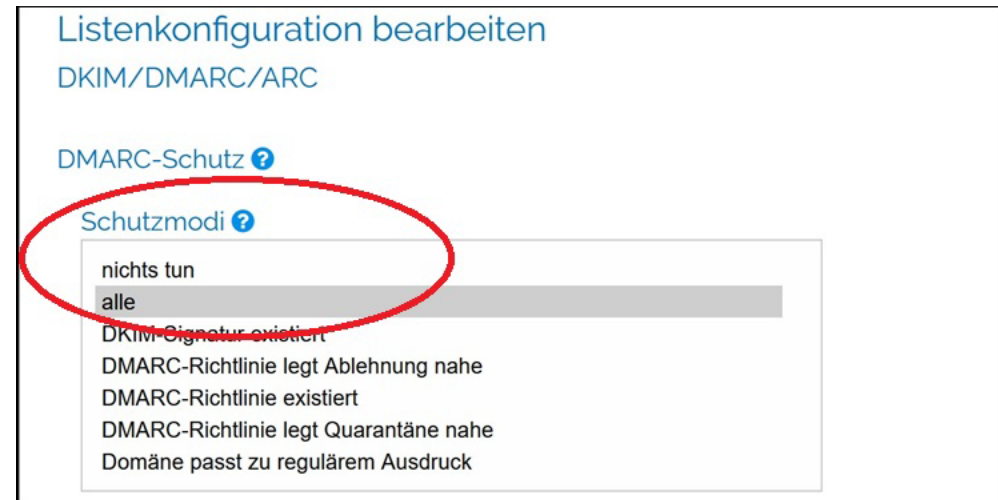
→ Ersetzung des From-Headers des ursprünglichen Absenders durch die Listenadresse
z.B. **From:** "Olaf Hopp" (via testliste Mailing List) <testliste@listserv.dfn.de>

Vorteile:

- Bessere Zustellbarkeit
- DKIM-Signatur vom DFN-Listserv

Nachteile:

- Absender ist nicht der ursprüngliche Absender
- Digitale S/MIME Signaturen werden ungültig

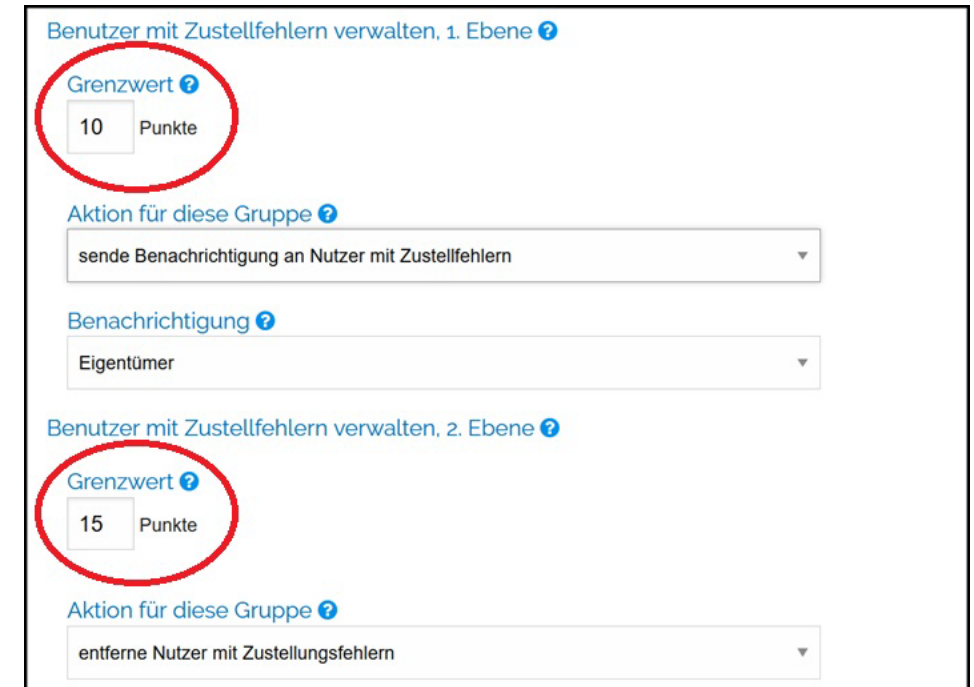


Empfehlungen zur Konfiguration von Mailinglisten

Automatisches Bounce-Handling:

- Sympa berechnet Zustellfehlerwert für E-Mail-Adressen mit mehreren Zustellfehlern.
- Beim Erreichen von zwei Grenzwerten werden Aktionen durchgeführt:
 1. Grenzwert: Informationsmail an die Listeneigentümer
 2. Grenzwert: Löschen der betroffenen E-Mail-Adressen
- Grenzwerte sind standardmäßig hoch angesetzt und sinnvoll für Listen mit vielen Postings;
bei Listen mit wenigen Postings werden die Grenzwerte nicht erreicht
- Pflege der Abonnentenliste ist wichtig für Reputation der Mailserver

Empfehlung: Grenzwerte für Listen mit wenig Mailverkehr herabsetzen



Benutzer mit Zustellfehlern verwalten, 1. Ebene ?

Grenzwert ?
10 Punkte

Aktion für diese Gruppe ?
sende Benachrichtigung an Nutzer mit Zustellfehlern

Benachrichtigung ?
Eigentümer

Benutzer mit Zustellfehlern verwalten, 2. Ebene ?

Grenzwert ?
15 Punkte

Aktion für diese Gruppe ?
entferne Nutzer mit Zustellungsfehlern



Karlsruher Institut für Technologie