Dienstbeschreibung DFN-MailSupport

1 Zweck dieser Dienstbeschreibung

Diese Dienstbeschreibung gibt einen grundlegenden Überblick über den Leistungsumfang des Dienstes DFN-MailSupport ab dem 1.12.2025 und stellt Voraussetzungen und Rahmenbedingungen für die Teilnahme an diesem dar.

Diese Dienstbeschreibung ergänzt inhaltlich die den Dienst DFN-MailSupport betreffenden Dokumente

- ✓ Entgeltordnung (DFN-MailSupport, Dienst-Paket),
- ✓ Rahmenvertrag und
- ✓ Dienstvereinbarung DFN-MailSupport

um technische Spezifikationen zur Realisierung und betrieblichen Ausführung.

Zur Sicherstellung dieser Anforderungen wird sie nach den Erfordernissen des DFN-Vereins und im Hinblick einer zeit-, bedarfs- und kostengerechten technischen Weiterentwicklung des Dienstes DFN-MailSupport im Interesse der Gemeinschaft der Mitglieder und Nutzenden erweitert und aktualisiert.

2 DFN-MailSupport auf einen Blick

Der DFN-Verein entwickelt, organisiert und betreibt mit DFN-MailSupport eine Dienstleistung, die das Aufkommen unerwünschter Inhalte[1] im E-Mailverkehr der Teilnehmer am Wissenschaftsnetz reduziert.

E-Mail ist ein zentraler Dienst für die Kommunikation aller Nutzenden im Wissenschaftsnetz. Die einwandfreie Funktion von E-Mails ist eine Grundlage vieler Prozesse in Forschung und

[1] Spam oder Malware (Viren, Würmer, Trojaner etc.)

Lehre. Bei der Verarbeitung von E-Mails sind nicht nur technische und organisatorische, sondern insbesondere auch datenschutzrechtliche und strafrechtliche Aspekte mit größter Sorgfalt zu beachten. Die Erbringung einer vertrauenswürdigen, rechtlich einwandfreien und qualitativ hochwertigen E-Mail-Filterlösung ist somit für alle wissenschaftlichen Einrichtungen eine tägliche Herausforderung.

Vor diesem Hintergrund haben sich die im DFN-Verein organisierten Einrichtungen dazu entschieden, dass ihre individuellen E-Mail-Dienste durch einen gemeinschaftlich geplanten Dienst unterstützt werden sollen.

2.1 Grundsätze bei der Erbringung des Dienstes

Um den Anforderungen an eine stabile und zuverlässige Dienstleistung gerecht zu werden, orientiert sich DFN-MailSupport an den folgenden Grundsätzen und Qualitätsanforderungen.

- **Vertraulichkeit**

Die Sensibilität der Daten erfordert höchste Vertraulichkeit und Integrität des Dienstes, denn jede E-Mail liegt vollständig und (sofern unverschlüsselt) im Klartext vor. Die vom DFN-Verein selbst betriebene Dienstumgebung hat das Ziel, den bestmöglichen Schutz der Daten zu gewährleisten.

- **Verfügbarkeit**

Der hohe Anspruch an die Verfügbarkeit von DFN-MailSupport wird durch den Einsatz geeignet dimensionierter und im Wissenschaftsnetz georedundant verteilter Systeme gewährleistet.

In Anlehnung an ISO 27001 auf der Basis von IT-Grundschutz werden insbesondere Maßnahmen zur Absicherung der Betriebsumgebung (IT-Sicherheit) intensiv betrachtet.

- **Zuverlässigkeit**

Der Dienst wird in enger Abstimmung mit den teilnehmenden Einrichtungen im Wissenschaftsnetz entwickelt und greift dadurch einrichtungsübergreifend auf langjährige Erfahrung und Know-how bezüglich der Maßnahmen zum Schutz vor unerwünschten E-Mails zurück. Zudem wird für kritische Komponenten, wie z. B. die Virenerkennung, auf Lösungen von verschiedenen Herstellern im Parallelbetrieb zurückgegriffen.

Die Erkennungsraten werden im internen Berichtswesen über längere Zeiträume hinweg erfasst und den Ergebnissen vergleichbarer Lösungen gegenübergestellt.

- **Rechtliche Absicherung**

Die Verarbeitung personenbezogener Daten, die Einsichtnahme in sowie die Weiterleitung von E-Mails unterliegen rechtlichen Vorgaben. Deshalb sind die Filterprozesse von DFN-MailSupport mit besonderer Sorgfalt entworfen worden und werden in regelmäßigen Abständen während eines Datenschutzaudits auf ihre rechtliche Konformität überprüft.

E-Mailinhalte werden grundsätzlich automatisiert verarbeitet und die Speicherung von Daten unterliegt sehr restriktiven Vorgaben. Situationen, in denen die Einsichtnahme unvermeidbar ist, sind streng reglementiert und werden dokumentiert.

E-Mails werden zu keinem Zeitpunkt gelöscht oder unterdrückt. DFN-MailSupport bewertet schadhafte bzw. unerwünschte Inhalte anhand von Bewertungskriterien und vergibt sogenannte Spam-Punkte, sobald in einer E-Mail entsprechende Inhalte auftreten. Die Summe der Spam-Punkte pro E-Mail ergibt den Spam-Score der Mail.

Die teilnehmende Einrichtung kann hierfür eigene Schwellwerte festlegen. Wird dieser Schwellwert bereits überschritten, während die E-Mail noch nicht vollständig eingeliefert wurde, wird der Empfang der betroffenen E-Mail abgelehnt und der Absender wird über den fehlgeschlagenen Einlieferungsversuch informiert. Wird die Überschreitung des Schwellwertes erst nach vollständiger Einlieferung erkannt, werden die Ergebnisse der Checks im Header-Teil der betroffenen E-Mail dokumentiert und die E-Mail selbst wird (ebenfalls im Header) als Spam markiert. Sie wird anschließend der Empfängereinrichtung zugestellt.

2.2 Leistungsumfang

Im Leistungsumfang von DFN-MailSupport sind enthalten:

- ✓ eine Sammlung unterschiedlicher und fein granular konfigurierbarer Filtermaßnahmen und -Werkzeuge für ein- und ausgehenden E-Mailverkehr
- ✓ technischer Support (2nd Level) und Beratung
- ✓ 24/7-Zugang zu einem Konfigurationsportal

Die Dienstumgebung von DFN-MailSupport unterwirft sich dem IT-Grundschutz-Kompendium des BSI. Aus diesem Grund sind zwei Informationsverbünde gegründet worden, die seit 2015 regelmäßigen Auditierungszyklen unterliegen.

Das Hosting der Postfächer einer teilnehmenden Einrichtung ist **nicht** im Leistungsumfang von DFN-MailSupport enthalten.

3 Nutzungsvarianten

DFN-MailSupport ist neben seiner Funktion als Filter eingehender E-Mails ebenfalls in der Lage, ausgehende E-Mails zu filtern.

3.1 Eingehender Filter

Die MX-Records der Domains einer teilnehmenden Einrichtung zeigen direkt auf die E-Mail-Gateways des DFN-Vereins. Die eingehenden E-Mails werden während des Empfangs geprüft. Anhand der Checkergebnisse werden sie abgelehnt oder angenommen. Angenommene E-Mails werden markiert oder – entsprechend den Einstellungen der teilnehmenden Einrichtung modifiziert – in deren Mailqueue abgelegt.

Die Zustellung der E-Mails erfolgt aus der Queue heraus an diejenigen Mailserver, die die betroffene Einrichtung pro Domain in ihrer Konfiguration hinterlegt hat.

3.2 Ausgehender Filter

Für das Filtern ausgehender E-Mails konfiguriert die teilnehmende Einrichtung die Mail-Gateways des DFN-Vereins als Relays in ihren Systemen. Hierzu stellt DFN-MailSupport einen speziellen MX-Record zur Verfügung.

Bevor dieselben Checks wie beim eingehenden Filtern erfolgen, findet ein Ratelimiting statt. Passiert eine E-Mail alle Checks, so wird sie optional DKIM-signiert und in der Mailqueue abgelegt. Anschließend wird die E-Mail – entsprechend der Teilnehmerkonfiguration vom DFN bzw. von der Teilnehmereinrichtung selbst – an die gewünschte Empfangsadresse versendet.

3.3 By-Pass-Betrieb zu Testzwecken

Es ist möglich, DFN-MailSupport so zu konfigurieren, dass dieselbe E-Mail gleichzeitig die Filterelemente von DFN-MailSupport, sowie einer weiteren Filterlösung passiert. Bei der Konfiguration ist allerdings darauf zu achten, dass es in der Empfangskette nur einen einzigen Mailserver geben darf, der in der Lage dazu ist, E-Mails abzulehnen.

Dieses Szenario wird häufig dann genutzt, wenn bspw. eine teilnehmende Einrichtung die Ergebnisse ihrer bestehenden Lösung für das E-Mail-Abuse-Management einer Alternative gegenüberstellen möchte. Der DFN-Verein bietet deshalb an, die eigenen Header mit „DFN“ zu kennzeichnen („X-Spam“ vs. „X-DFN-Spam“).

Auch wenn hier das Testen im Vordergrund steht und die Entscheidung, ob die interessierte Einrichtung künftig am Dienst DFN-MailSupport teilnehmen möchte, erst noch gefällt werden muss, ist es zwingend erforderlich, dass die vertraglichen Dokumente (siehe Abschnitt 5 *Nutzungsvoraussetzungen*) vor der Inbetriebnahme anerkannt worden sind.

3.4 DFN-MailSupport in Verbindung mit GWDG – Open-Xchange

Einrichtungen, die den föderierten Dienst GWDG – Open-Xchange aus der DFN-Cloud einsetzen, verwenden automatisch DFN-MailSupport als Filterlösung und unterliegen damit ebenfalls den Anforderungen aus den Nutzungsvoraussetzungen (siehe Abschnitt 5).

4 Betrieb

Grundsätzlich steht es einer teilnehmenden Einrichtung frei, ob sie nur eine einzige der von ihr betriebenen E-Mail-Domains, eine Untermenge davon oder alle E-Mail-Domains von DFN-MailSupport filtern lässt.

Immer dann, wenn sich die Filterprozesse zwischen zwei E-Mail-Domains unterscheiden sollen, verwendet DFN-MailSupport das Prinzip separater Instanzen. Alle E-Mail-Domains innerhalb einer Instanz werden mit denselben Filtereigenschaften versorgt.

4.1 Inbetriebnahme

Sobald anhand der Angaben aus dem technischen Formblatt die individuelle Konfiguration im System abgebildet worden ist, erhält die teilnehmende Einrichtung ihre neuen MX-Records, von denen sie künftig den gefilterten E-Mailverkehr empfängt. Der DNS-Eintrag für die E-Mail-Domains verbleibt zu jedem Zeitpunkt in der Verantwortung der teilnehmenden Einrichtung. Dadurch kann die Nutzung von Teilnehmerseite aus zu jedem Zeitpunkt unterbrochen und wieder aufgenommen werden.

Weitere Details zur Erstkonfiguration sowie Erläuterungen zur E-Mailverarbeitung, eingefügten E-Mail-Headern und Handlungsempfehlungen finden Sie in unserer Online-Doku.

4.2 Interaktives Konfigurationsportal

Die konkreten Einstellungen einer individuellen Instanz pflegt die teilnehmende Einrichtung über das Konfigurationsportal, welches ihr der DFN-Verein mit dem Dienst DFN-MailSupport zur Verfügung stellt. Für den Zugang zum Konfigurationsportal ist die Teilnahme an der DFN-AAI notwendig. Weitere Informationen zum Konfigurationsportal entnehmen Sie bitte der Online-Doku.

Alternativ können alle Parameter ebenfalls mithilfe der unter Abschnitt 7 *Entstörung* genannten technischen Hotline gesteuert werden.

4.3 Betriebsumgebung

Die E-Mail-Gateways, die für DFN-MailSupport eingesetzt werden, befinden sich an den X-WiN-Kernnetzknoten HAN, TUB und ERL.

Die Standorte sind identisch ausgestattet und deren Leistungsfähigkeit wurde so gewählt, dass auch bei einem Ausfall zweier Standorte der komplette E-Mailverkehr temporär durch den verbliebenen dritten Standort aufgefangen werden kann.

4.4 Log-Daten-Analyse

Das DFN-CERT analysiert Security Events aus angefallenen Log-Daten und kann daraus Informationen zur Erkennung und Alarmierung im Umfeld der DFN-Dienste entnehmen. Das angestrebte Ziel ist die Verbesserung eines ganzheitlichen Sicherheitslagebildes, das nicht nur die einzelnen DFN-Dienste sondern auch die Gesamtinfrastruktur umfasst.

Die Nutzenden von DFN-MailSupport werden bei Abschluss der Dienstvereinbarung darüber informiert, dass das DFN-CERT Log-Daten des Dienstes für die o. g. Zwecke verarbeitet.

4.5 Ham- und Spam-Training

Spaminhalte verändern sich fortlaufend. Während bei regelbasierten Filtern analog zu Virenfiltern die Regeln von Hand angepasst werden müssen, können sich statistische Filter selbst adaptieren. Voraussetzung hierfür ist allerdings regelmäßiges Training mit manuell klassifizierten Spam- und Ham-Mails. Dieses Training wird durch die Administratoren des DFN-MailSupport-Dienstes durchgeführt. Die Durchführung beinhaltet ein manuelles Review der Spam-Trainingsergebnisse.

Interessierte Postmaster möchten wir dazu ermutigen, am Training teilzunehmen. Bitte kontaktieren Sie die Hotline, um die Trainingsadressen für Ihre Einrichtung konfigurieren zu lassen.

Teilnehmende Einrichtungen können per Dienstvereinbarung regeln, ob Sie automatisiertem Spam- und Ham-Training in Form von stichprobenartigen Entnahmen von E-Mails aus dem regulären Datenstrom zustimmen möchten oder nicht.

5 Nutzungsvoraussetzungen

DFN-MailSupport steht ausschließlich den Einrichtungen zur Verfügung, die über einen DFN-Internetanschluss **oder** ein Dienst-Paket verfügen.

Vor der initialen Inbetriebnahme von DFN-MailSupport müssen am Dienst teilnehmende Einrichtungen mit dem DFN-Verein eine Dienstvereinbarung sowie eine Rahmen-Auftragsverarbeitungsvereinbarung (Rahmen-AVV) inklusive einem dienstspezifischen Anhang zur Rahmen-AVV für DFN-MailSupport abschließen.

Zusätzlich werden technische Parameter zur E-Mailinfrastruktur der teilnehmenden Einrichtung im Rahmen eines technischen Formblattes abgefragt.

Die Anerkennung dieser Dokumente ist für alle Nutzungsarten von DFN-MailSupport – einschließlich für Test- und Vergleichszwecke – erforderlich.

Zum Abruf des Vertragswerks bzw. bei Fragen dazu, wenden Sie sich bitte an unsere Vertragshotline.

6 Support & Entstörung

Erreichbarkeit der technischen Hotline:

- ✓ wochentags von 9-12 Uhr und von 14-17 Uhr

Bitte beachten Sie die regionalen Feiertage in Baden-Württemberg.

7 Weitere Informationen

Der Dienst DFN-MailSupport ist so konzipiert, dass seine Bestandteile sehr genau an die Bedürfnisse teilnehmender Einrichtungen angepasst werden können. Insbesondere im Umfeld von Wissenschaft und Forschung existieren Nutzungsszenarien, die sich von der E-Mailkommunikation anderer Nutzergruppen unterscheiden. Die Entscheidung, ob ein Inhalt erwünscht oder unerwünscht ist, wird einrichtungsübergreifend aufgrund sehr unterschiedlicher Kriterien und Schwellwerte getroffen.

Deshalb ist DFN-MailSupport modular aufgebaut und gibt teilnehmenden Einrichtungen sehr viele Konfigurationsparameter für ihre eigene Dienstnutzung an die Hand. Eine Erklärung der entsprechenden Dienstparamater, Angaben zu Default-Werten und Informationen zur Software-Umsetzung sowie allen konkreten Dienstkomponenten und Filterbestandteilen finden Sie in der Online-Doku von DFN-MailSupport.

8 Anhang Glossar

Eine umfangreiche und aktuelle Sammlung der im Text markierten Begriffe und Begriffserklärungen rund um DFN-MailSupport finden Sie auf unseren Webseiten unter: www.mailsupport.dfn.de/glossar

A. Anhang Änderungshistorie

Version	Datum	Änderungen
1.0	November 2025	Initiale Version