VAUTRON
RECHENZENTRUM AG

mailrepo.de — Kundenhandbuch

März 2026 · Version 1.0

Vautron Rechenzentrum AG

Inhaltsverzeichnis

1 Was ist mailrepo.de?

mailrepo.de ist ein E-Mail-Archivierungsdienst für Unternehmen. Er unterstützt die Einhaltung gesetzlicher Aufbewahrungspflichten (z. B. GoBD, HGB §§ 238, 257).

Nach einmaliger Einrichtung werden ein- und ausgehende E-Mails automatisch archiviert, verschlüsselt, manipulationsgeschützt protokolliert und über eine intelligente Suche auffindbar gemacht — ohne manuellen Eingriff.

2 Kernprinzipien

- **Ende-zu-Ende-Verschlüsselung:** Der Server hat zu keinem Zeitpunkt Zugriff auf den Klartext Ihrer E-Mails. Die Entschlüsselung findet ausschließlich in Ihrem Browser statt.
- **Manipulationssicherheit:** Jede archivierte E-Mail wird in einer kryptographischen Audit-Kette mit unabhängigen Zeitstempeln gesichert.
- **Automatisierung:** Nach einmaliger Einrichtung läuft die Archivierung vollautomatisch.
- **Datensparsamkeit:** Nur die für den Betrieb notwendigen Daten werden gespeichert.

3 Wie funktioniert die Archivierung?

4 Übersicht

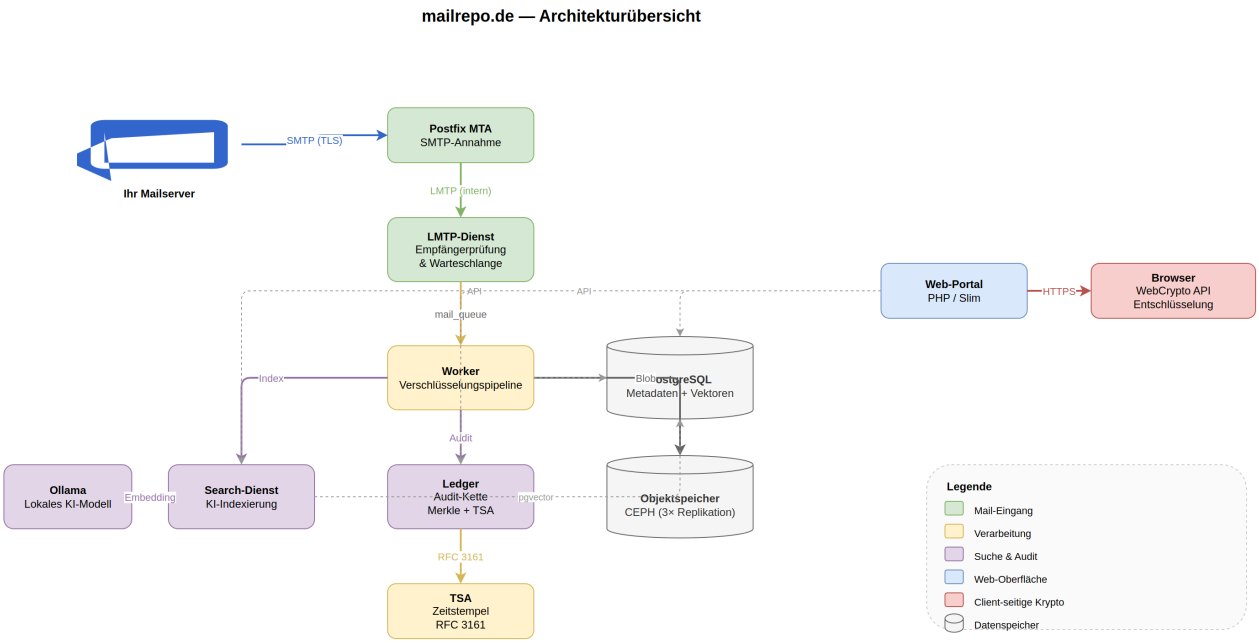


Abbildung 1: Architekturübersicht

Sie konfigurieren Ihren Mailserver so, dass er eine Kopie jeder ein- und ausgehenden Mail per SMTP an mailrepo.de weiterleitet. Ab diesem Punkt läuft alles automatisch:

1. **Empfang:** Ihr Mailserver sendet die Mail per SMTP an mailrepo.de.
2. **Komprimierung & Verschlüsselung:** Die Mail wird zunächst komprimiert (gzip) um Speicherplatz zu sparen und anschließend mit einem zufällig erzeugten Schlüssel verschlüsselt. Dieser Schlüssel wird wiederum mit Ihrem persönlichen öffentlichen Schlüssel gesichert (Details in Kapitel 3).
3. **Speicherung:** Der verschlüsselte Inhalt wird auf einem verteilten Speichersystem mit dreifacher Replikation abgelegt.
4. **Protokollierung:** Ein kryptographischer Eintrag in der Audit-Kette beweist Zeitpunkt und Inhalt der Archivierung (Details in Kapitel 5).
5. **Indexierung:** Die Mail wird für die semantische Suche aufbereitet — ohne den Klartext zu speichern (Details in Kapitel 6).

5 Mail-Zustellungsablauf

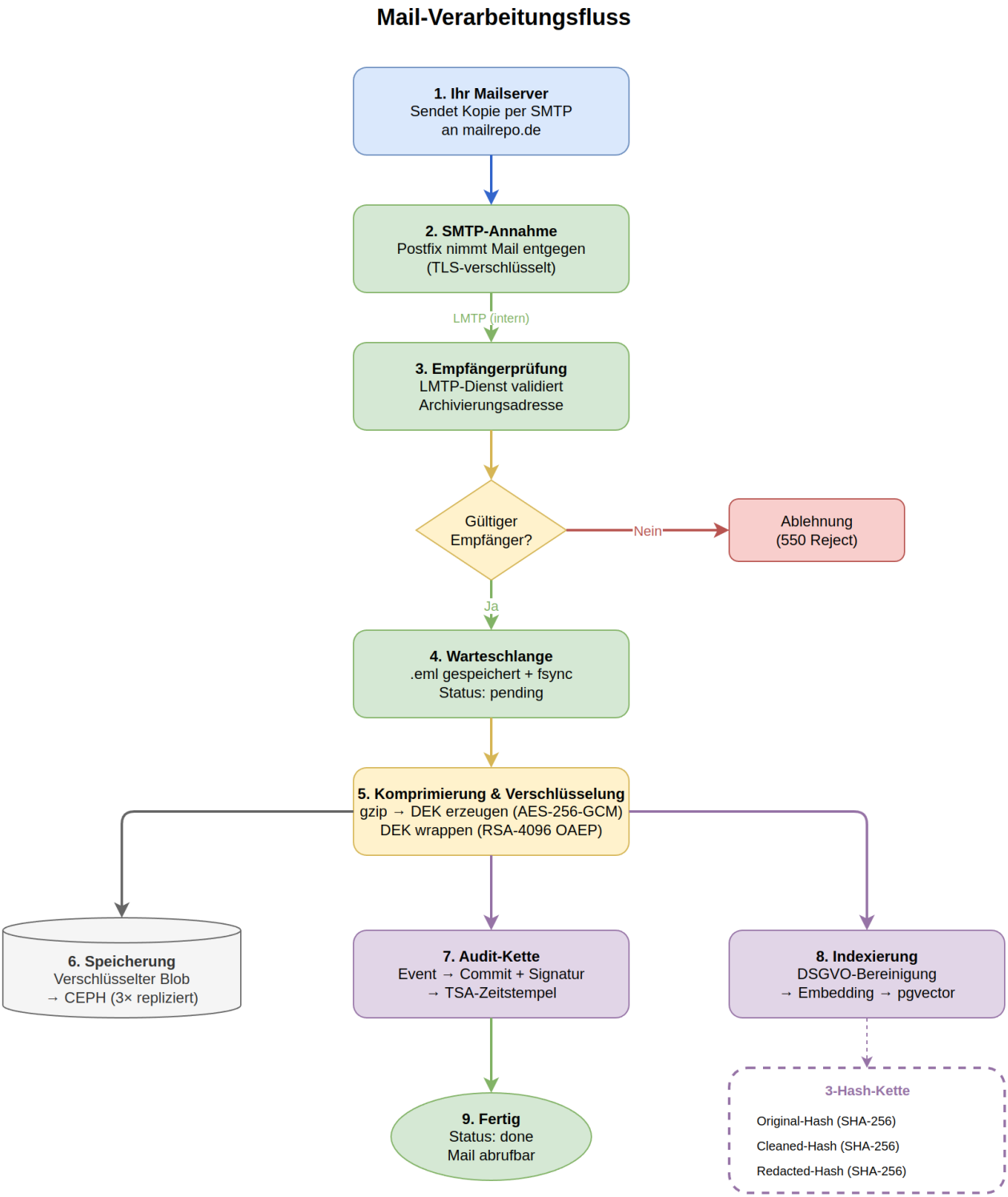
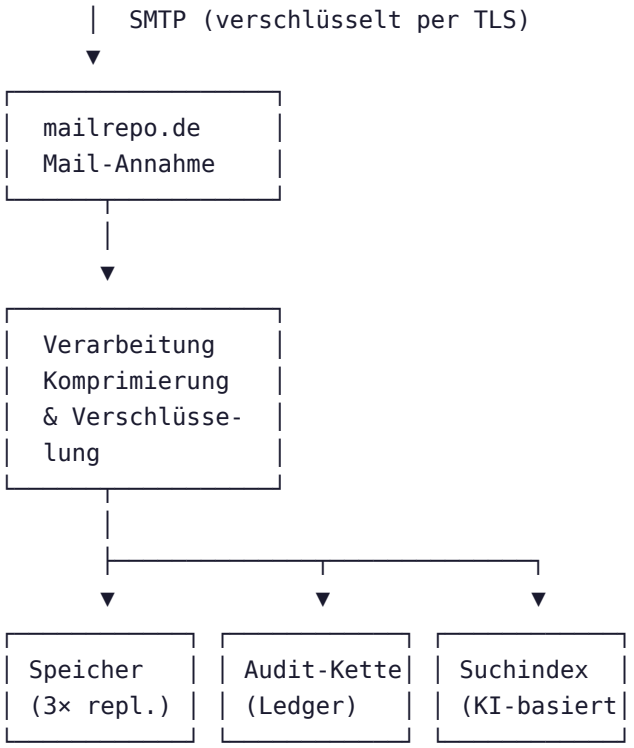


Abbildung 2: Mail-Verarbeitungsfluss

```
Ihr Mailserver
      |
```



6 Adressformat

Ihre Archivierungsadresse folgt einem festen Schema:

`archive-vautron-<kundennummer>@mailrepo.de`

Optionale Tags zur Kategorisierung (z. B. Abteilungen) hängen Sie mit + an:

`archive-vautron-<kundennummer>+buchhaltung@mailrepo.de`

---

7 Sicherheit & Verschlüsselung

8 Zero-Knowledge-Prinzip

Das Sicherheitsmodell basiert auf dem **Zero-Knowledge-Prinzip:** Der Server speichert und verarbeitet ausschließlich verschlüsselte Daten. Die Entschlüsselung findet ausschließlich im Browser des Kunden statt. Weder der Betreiber noch ein Administrator kann Ihre E-Mails lesen.

9 Schlüsselhierarchie

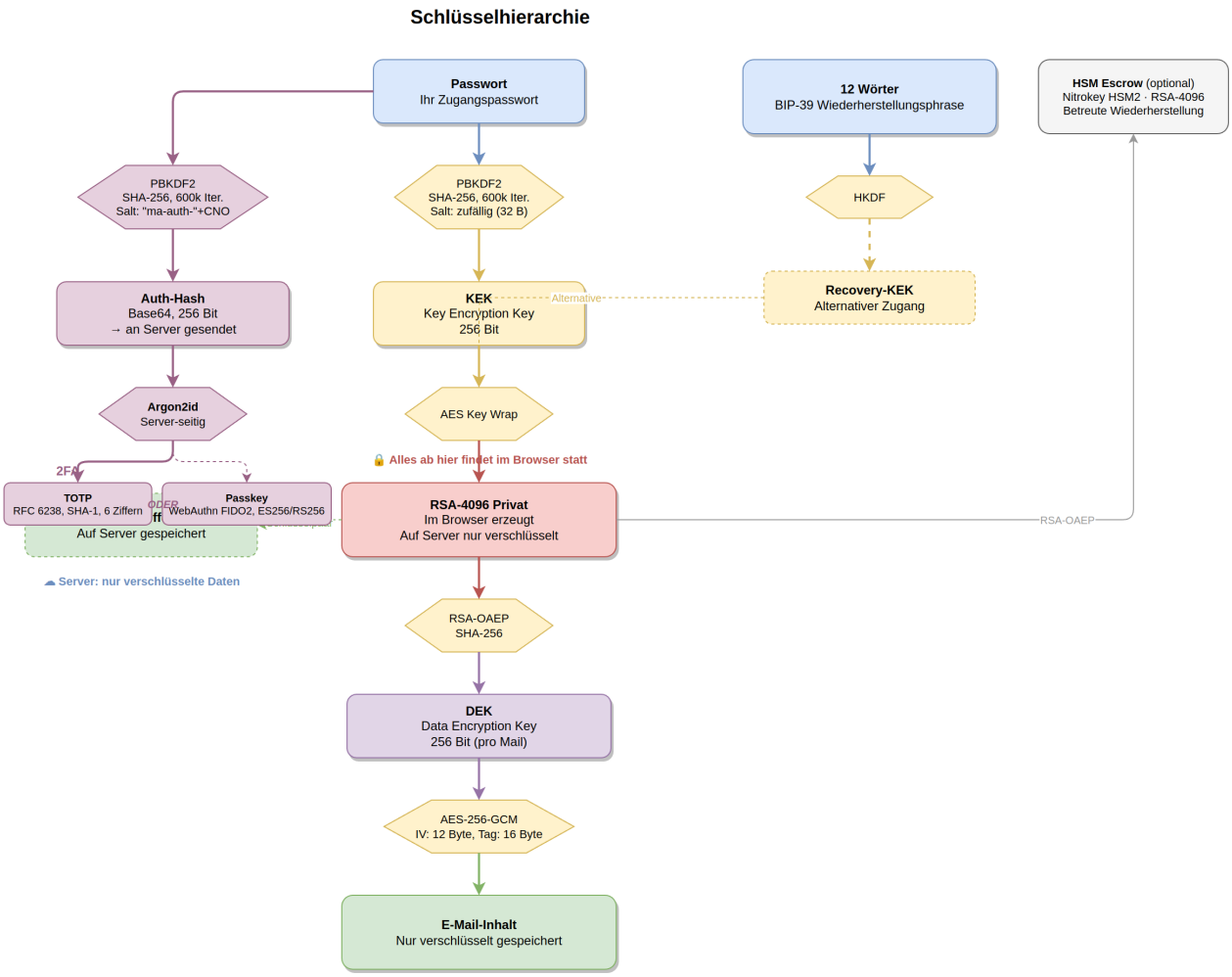
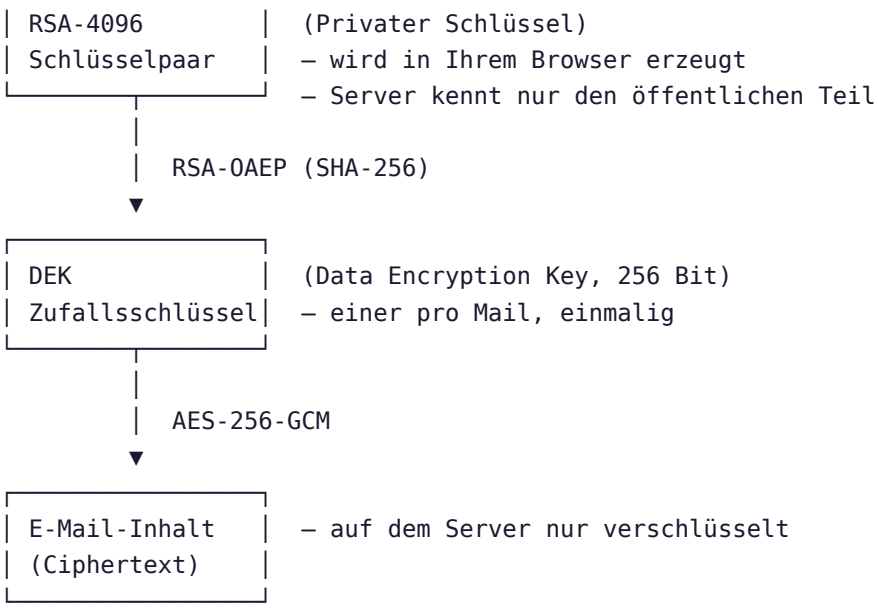


Abbildung 3: Schlüsselhierarchie

Ihre E-Mails werden über eine mehrstufige Schlüsselhierarchie geschützt:

```
Ihr Passwort
    │
    ├── PBKDF2 ("ma-auth-"+CNO, 600.000 Iter.)
    │   ▼
    │   Auth-Hash ──────────────► Server (sichere Prüfung)
    │
    │   PBKDF2 (zufälliger Salt, 600.000 Iterationen)
    ▼
┌──────────────────┐
│ KEK              │  (Key Encryption Key, 256 Bit)
│ AES Key Wrap     │  – schützt Ihren privaten Schlüssel
└──────────────────┘  – verbleibt im Browser, wird NIE übertragen
        │
        ▼
┌──────────────────
```



10 Verschlüsselungsalgorithmen im Detail

Ebene	Algorithmus	Parameter	Zweck
Mail-Inhalt	AES-256-GCM	256-Bit-Schlüssel, 12-Byte-IV, 16-Byte-Tag	Verschlüsselung der E-Mail
DEK-Wrapping	RSA-OAEP	4096-Bit RSA, SHA-256	Verschlüsselung des Mail-Schlüssels
Privater Schlüssel	AES Key Wrap	256-Bit KEK	Schutz des privaten Schlüssels
KEK-Ableitung	PBKDF2	SHA-256, 600.000 Iterationen, 16-Byte-Salt	Passwort → Schlüssel
Recovery-KEK	HKDF	BIP-39 Entropy → Key	Alternative Schlüsselableitung
Ledger-Signatur	Ed25519 / ECDSA P-256 / ML-DSA-65	Variabel	Signierung der Audit-Kette
Zeitstempel	RFC 3161 TSA	Extern	Unabhängiger Zeitnachweis

11 Entschlüsselungsprozess

Beim Öffnen einer Mail im Web-Portal passiert Folgendes — alles in Ihrem Browser:

1. Der verschlüsselte Mail-Inhalt wird vom Server geladen.
2. Der verschlüsselte Schlüssel (DEK) wird vom Server geladen.
3. Ihr Passwort wird per PBKDF2 zum KEK abgeleitet.
4. Der KEK entpackt Ihren privaten RSA-Schlüssel.
5. Der private RSA-Schlüssel entpackt den DEK.

6. Der DEK entschlüsselt die Mail per AES-256-GCM.
7. Falls komprimiert, wird die Mail automatisch dekomprimiert (gzip).
8. Die entschlüsselte Mail wird im Browser dargestellt — sie verlässt nie Ihren Rechner.

All diese Schritte werden von der **WebCrypto API** durchgeführt — einer standardisierten Kryptographie-Schnittstelle Ihres Browsers.

12 Wiederherstellungsphrase (12 Wörter)

Bei der Ersteinrichtung erhalten Sie eine **12-Wort-Wiederherstellungsphrase** (nach BIP-39-Standard). Diese Phrase ist ein alternatives Backup Ihres privaten Schlüssels.

Wichtig: Die Wiederherstellungsphrase ist der einzige Weg, den Zugriff auf Ihre Mails wiederherzustellen, wenn Sie Ihr Passwort vergessen. Der Betreiber hat keinen Zugriff auf Ihren privaten Schlüssel und kann keine Entschlüsselung für Sie durchführen.

> **Optional: HSM-Escrow**
> Auf Wunsch kann Ihr privater Schlüssel zusätzlich mit einem zertifizierten Hardware-Sicherheitsmodul (HSM, Nitrokey HSM2) verschlüsselt hinterlegt werden. Dies ermöglicht eine betreute Wiederherstellung im Notfall — auch wenn Sie sowohl Passwort als auch Wiederherstellungsphrase verloren haben. Der Betreiber kann Ihren Schlüssel nur mit physischem Zugriff auf das HSM und dem HSM-PIN entschlüsseln. Die Aktivierung erfolgt während der Ersteinrichtung oder nachträglich in den Einstellungen.

13 Authentifizierung

Maßnahme	Details
Passwort	Ihr Passwort verlässt nie Ihren Browser — es wird lokal in einen Auth-Hash umgewandelt und nur dieser an den Server gesendet. Dort wird er zusätzlich mit Argon2id gehasht.
TOTP (2FA)	Zeitbasiertes Einmalpasswort, 30-Sekunden-Intervall
Passkeys	Phishing-resistente Alternative zum TOTP-Code. Nutzt den Fingerabdrucksensor, Face ID oder einen USB-Sicherheitsschlüssel Ihres Geräts (FIDO2/WebAuthn).
Backup-Codes	Einmalige Notfall-Codes bei Verlust des TOTP-Geräts
Kontosperre	Nach 5 Fehlversuchen für 15 Minuten gesperrt
Sitzungsschutz	Sitzungen gebunden an IP und Browserkennung

---

14 Web-Portal — Ihr Zugang zum Archiv

15 Dashboard

Nach der Anmeldung sehen Sie auf einen Blick:

- Gesamtanzahl archivierter Mails und Eingänge des heutigen Tages
- Speicherverbrauch und Kontingent
- Mail-Volumen der letzten 30 Tage als Diagramm
- Verteilung nach Status und Top-Empfänger

16 Mail-Suche

- **Semantische Suche:** KI-basierte Ähnlichkeitssuche versteht Synonyme und verwandte Begriffe — Sie finden, was Sie meinen, nicht nur was Sie tippen.
- **Chronologische Suche:** Sortierung nach Datum, Filterung nach Zeitraum, Status, Tag, Empfänger und Größe.
- **Mail-Detailansicht:** Entschlüsselung und Darstellung direkt im Browser.

17 Audit-Kette (Ledger)

- Anzeige der kryptographischen Einträge für Ihre archivierten Mails
- Integritätsprüfung einzelner Mails
- Zeitstempel der unabhängigen Zeitstempelstelle anzeigen

18 Löschprotokoll

- Übersicht aller gelöschten Mails
- Zeitstempel, Benutzer und Löschgrund für jede Löschung

19 Einstellungen

- **TOTP-Verwaltung:** Einrichtung und Verwaltung Ihrer Zwei-Faktor-Authentifizierung. Sie können mehrere Authenticator-Geräte registrieren oder Ihr TOTP-Secret zurücksetzen.
- **Passkeys:** Passkeys als phishing-resistente Alternative zum TOTP-Code hinzufügen, umbenennen oder entfernen (FIDO2/WebAuthn)
- **Backup-Codes:** Generierung einmaliger Notfall-Codes für den Fall, dass Ihr Authenticator-Gerät nicht verfügbar ist
- **Wiederherstellungsphrase:** Anzeige Ihrer 12-Wort-Phrase oder Regenerierung einer neuen Phrase (die alte wird dabei ungültig)
- **Schlüsselexport:** Export Ihres verschlüsselten privaten Schlüssels
- **Sitzungsverwaltung:** Übersicht aktiver Sitzungen und Remote-Abmeldung
- **DSGVO-Datenexport:** Download aller über Sie gespeicherten Daten als ZIP
- **Passwortänderung:** Automatisches Re-Wrapping Ihres Schlüssels

20 Hilfe & FAQ

In der Hilfe finden Sie u. a.:

- Einführung und Erste Schritte
- Sicherheitsmodell erklärt
- Entschlüsselungsprozess Schritt für Schritt
- FAQ mit den häufigsten Fragen
- Glossar technischer Begriffe

---

21 Manipulationssicherheit — Die Audit-Kette

22 Was beweist die Audit-Kette?

Jede archivierte E-Mail erhält einen fälschungssicheren Eintrag in einer kryptographischen Audit-Kette (Ledger). Dieser Eintrag beweist:

- **Wann** die Mail archiviert wurde — mit einem unabhängigen Zeitstempel (RFC 3161 TSA)
- **Was** archiviert wurde — über den kryptographischen Hash des Inhalts (SHA-256)
- **Dass** die Reihenfolge nicht verändert wurde — über eine verkettete Hash-Kette

23 Für-Ebenen-Hierarchie

Die Audit-Kette organisiert ihre Einträge in vier Ebenen:

24 Ebene 1 — Events (pro Mail)

Jede Mail erzeugt einen Eintrag mit dem Hash des Inhalts, der Dateigröße und einem Zeitstempel. Jeder Eintrag verweist auf den vorherigen und bildet so eine unveränderliche Kette.

25 Ebene 2 — Commits (Batch-Zusammenfassung)

Mehrere Events werden periodisch zu einem Commit zusammengefasst: - Ein **Merkle-Baum** (RFC 6962) fasst alle Events in einem einzigen Hash zusammen. - Der Commit wird **digital signiert** (Ed25519, ECDSA P-256 oder ML-DSA-65). - Ein **RFC 3161 Zeitstempel** einer unabhängigen Zeitstempelstelle wird angehängt.

26 Ebene 3 — Tenant Heads (pro Mandant)

Commits werden pro Mandant zu einer Zusammenfassung aggregiert.

27 Ebene 4 — Root Heads (global)

Alle Mandanten-Zusammenfassungen werden zu einem globalen Integritätsanker zusammengefasst.

28 Merkle-Beweis (Einzelnachweise)

Für jede einzelne Mail kann ein **Merkle-Beweis** erzeugt werden. Dieser belegt, dass eine bestimmte Mail Teil eines signierten und zeitgestempelten Commits ist — ohne die Inhalte anderer Mails offenzulegen.

Ein Merkle-Beweis enthält: - Den Hash der betreffenden Mail - Die Geschwister-Hashes im Merkle-Baum - Die digitale Signatur des Commits - Den TSA-Zeitstempel

Dieser Beweis ist **offline verifizierbar** — er benötigt keinen Zugang zum Archiv-System.

29 Post-Quantum-Sicherheit

Der Ledger unterstützt bereits **ML-DSA-65** (ehemals CRYSTALS-Dilithium), einen post-quanten-sicheren Signaturalgorithmus. Dieser schützt die Integrität der Audit-Kette auch gegen zukünftige Quantencomputer.

30 Kryptographische Algorithmen

Zweck	Algorithmus	Schlüssellänge
Hashing	SHA-256	256 Bit
Signatur	Ed25519 / ECDSA P-256 / ML-DSA-65	256 / 256 / PQC
Zeitstempel	RFC 3161 TSA	extern

---

31 Suche im Archiv

32 Semantische Suche

Die Suche in mailrepo.de funktioniert nicht wie eine klassische Volltextsuche, sondern nutzt **KI-basierte Ähnlichkeitssuche:**

- Sie finden Mails, auch wenn Sie nicht die exakten Worte kennen, die in der Mail vorkommen.
- Synonyme und verwandte Begriffe werden erkannt.
- Die Suche „versteht" die Bedeutung Ihrer Anfrage.

33 Wie funktioniert das ohne Klartext?

Die E-Mails werden nicht als Text im Suchindex gespeichert. Stattdessen:

1. Die Mail wird beim Eingang in **numerische Vektoren** (Zahlenwerte) umgewandelt, die die Bedeutung abbilden.
2. Nur diese Vektoren werden gespeichert — eine Rekonstruktion des Originaltexts ist nach aktuellem Stand der Technik nicht möglich.
3. Bei einer Suchanfrage wird Ihr Suchtext ebenfalls in einen Vektor umgewandelt und mit allen gespeicherten Vektoren verglichen.

34 Datenschutz bei der Indexierung

Vor der Vektorerzeugung werden automatisch sieben Kategorien personenbezogener Daten erkannt und entfernt:

1. Passwörter und Zugangsdaten
2. API-Schlüssel und Tokens
3. IBANs und Bankdaten
4. Telefonnummern
5. Postadressen
6. E-Mail-Adressen
7. Kundennummern

Die KI-Verarbeitung findet vollständig lokal statt — kein E-Mail-Inhalt verlässt das Rechenzentrum.

35 Drei-Hash-Nachverfolgung

Für jede Mail werden drei kryptographische Hashes berechnet, die die Datenminimierung nachvollziehbar machen:

Hash	Zeitpunkt	Zweck
Original-Hash	Nach dem Empfang	Verifizierung der Quelldaten
Cleaned-Hash	Nach der Normalisierung	Nachvollziehbarkeit der Bereinigung
Redacted-Hash	Nach der Datenschutz-Bereinigung	Nachweis der Datenminimierung

---

36 Aufbewahrung & Löschung

37 Automatische Aufbewahrung

Archivierte Mails werden gemäß den konfigurierten Aufbewahrungsfristen gespeichert. Nach Ablauf der Frist erfolgt die Löschung automatisch in zwei Stufen:

1. **Soft Delete:** Die Mail wird als gelöscht markiert.
2. **Endgültige Bereinigung:** Nach einer Karenzzeit werden der verschlüsselte Inhalt, die Schlüssel, die Suchvektoren und die Metadaten unwiderruflich entfernt.

38 Aufbewahrungsfrist ändern (Professional-Plan)

Im Professional-Plan können Sie die Aufbewahrungsfrist unter **Einstellungen → Aufbewahrungsfrist** selbst anpassen (365–36 500 Tage). Vor der Änderung wird Ihnen angezeigt, wie viele Mails betroffen wären.

Als Sicherheitsmaßnahme müssen Sie drei Faktoren bestätigen:

1. Ihr **Passwort**
2. Einen gültigen **TOTP-Code** — oder einen registrierten **Passkey**
3. Den Zustimmungstext wörtlich eintippen: *„Ich stimme der Änderung der Aufbewahrungsfrist zu"*

Im Basis-Plan ist die Aufbewahrungsfrist nur über den Support änderbar.

39 Manuelle Löschung

Die manuelle Löschfunktion ist standardmäßig deaktiviert und muss individuell für Ihr Konto freigeschaltet werden. Nach Freischaltung können einzelne Mails über die Detailansicht im Web-Portal zum Löschen vorgemerkt werden.

40 Dokumentation

Alle Löschvorgänge werden im Löschprotokoll mit Zeitstempel, Benutzer und Grund dokumentiert. Die Audit-Kette berücksichtigt Löschungen über ein Generationen-System (siehe Kapitel 5).

---

41 Datenschutz & DSGVO

42 Datenminimierung

- Nur für den Betrieb notwendige Metadaten werden gespeichert
- E-Mail-Inhalte sind ausschließlich verschlüsselt vorhanden
- Der Suchindex enthält nur numerische Vektoren, keine Texte
- IP-Adressen in Exports werden automatisch anonymisiert
- Sensible Felder werden in Protokollen automatisch geschwärzt

43 Standort

Alle Daten werden in einem **deutschen Rechenzentrum** verarbeitet und gespeichert. Es findet keine Übertragung in Drittländer statt.

44 Recht auf Auskunft (Art. 15 DSGVO) und Datenportabilität (Art. 20 DSGVO)

Unter **Einstellungen → Datenexport** können Sie alle über Sie gespeicherten Daten als ZIP-Datei herunterladen. Der Export enthält:

- Benutzerprofil (ohne Passwort)
- TOTP-Geräte (nur Namen)
- Passkeys (nur Namen und Erstellungsdatum)
- Login-Verlauf (letzte 100 Einträge)
- Aktive Sitzungen
- Öffentlicher Schlüssel
- Vollständiges Audit-Log
- Ledger-Statistiken, aktueller Ledger-Head und Kettenverifizierung
- Event-Detail-Ansicht: Klick auf einen Commit zeigt alle zugehörigen Journal-Events

IP-Adressen werden im Export automatisch anonymisiert.

45 Recht auf Löschung (Art. 17 DSGVO)

- Einzelne Mails können über die Detailansicht zum Löschen vorgemerkt werden.
- Gelöschte Mails werden in einem zweistufigen Prozess endgültig bereinigt.
- In der Audit-Kette wird der Löschvorgang korrekt über das Generationen-System berücksichtigt.
- Alle Löschvorgänge werden im Löschprotokoll dokumentiert.

46 Audit-Trail

Folgende Aktionen werden protokolliert:

Aktion	Protokolliert
Login (erfolg/fehlgeschlagen)	Zeitstempel, IP (anonymisiert), Browserkennung
Mail-Entschlüsselung	Zeitstempel, Mail-ID
Mail-Löschung	Zeitstempel, Mail-ID, Grund
Einstellungsänderung	Zeitstempel, Aktion
Passwortänderung	Zeitstempel

Das Audit-Log kann als CSV oder PDF exportiert werden.

---

47 Erste Schritte

48 Anmeldung

Öffnen Sie `https://www.mailrepo.de` und melden Sie sich mit Ihren Zugangsdaten an.

49 Einrichtungsassistent

Bei der ersten Anmeldung führt Sie ein dreistufiger Assistent durch die Einrichtung:

1. **TOTP einrichten:** Scannen Sie den QR-Code mit einer Authenticator-App (z. B. Google Authenticator, Authy) und bestätigen Sie mit einem generierten Code. Anschließend können Sie unter **Einstellungen → Passkeys** einen Passkey als Alternative zum TOTP-Code hinzufügen.
2. **Verschlüsselungsschlüssel erzeugen:** Ihr Browser erzeugt automatisch ein RSA-4096-Schlüsselpaar. Der private Schlüssel wird mit Ihrem Passwort geschützt (PBKDF2, 600.000 Iterationen).
3. **Wiederherstellungsphrase notieren:** 12 BIP-39-Wörter werden angezeigt. **Schreiben Sie diese auf und bewahren Sie sie sicher auf** — sie sind Ihr letztes Backup.

50 Mailserver konfigurieren

Konfigurieren Sie Ihren Mailserver so, dass er eine Kopie jeder ein- und ausgehenden Mail per SMTP an Ihre Archivierungsadresse weiterleitet. Die Verbindung muss per **TLS** gesichert sein (Port 25 mit STARTTLS oder Port 587).

51 Ihre Archivierungsadresse

Das Grundformat lautet:

`archive-vautron-<kundennummer>@mailrepo.de`

Optional können Sie **Tags** zur Kategorisierung anhängen — z. B. um Abteilungen, Domains oder Standorte zu unterscheiden:

```
archive-vautron-<kundennummer>+buchhaltung@mailrepo.de
archive-vautron-<kundennummer>+vertrieb@mailrepo.de
archive-vautron-<kundennummer>+example-com@mailrepo.de
archive-vautron-<kundennummer>+standort-berlin@mailrepo.de
```

Welches Tag-Schema am besten passt, entscheiden Sie. Im Web-Portal unter **Mail-Einrichtung** finden Sie einen Konfigurations-Generator, der die passenden Einstellungen für Ihren Mailserver erzeugt.

52 Postfix

Für **alle Mails** (ein- und ausgehend) eine BCC-Kopie senden:

```
# /etc/postfix/main.cf
always_bcc = archive-vautron-100123@mailrepo.de
```

Für **nur ausgehende Mails** (nach Absender):

```
# /etc/postfix/main.cf
sender_bcc_maps = hash:/etc/postfix/sender_bcc
```

```
# /etc/postfix/sender_bcc
@example.com    archive-vautron-100123+ausgehend@mailrepo.de
```

Für **nur eingehende Mails** (nach Empfänger):

```
# /etc/postfix/main.cf
recipient_bcc_maps = hash:/etc/postfix/recipient_bcc
```

```
# /etc/postfix/recipient_bcc
@example.com    archive-vautron-100123+eingehend@mailrepo.de
```

Für **mehrere Domains** mit getrennten Tags:

```
# /etc/postfix/sender_bcc
@firma-a.de     archive-vautron-100123+firma-a@mailrepo.de
@firma-b.de     archive-vautron-100123+firma-b@mailrepo.de
```

Nach jeder Änderung: `postmap /etc/postfix/sender_bcc && systemctl reload postfix`

TLS erzwingen: Damit die BCC-Kopie verschlüsselt übertragen wird, fügen Sie in `/etc/postfix/main.cf` hinzu:

```
smtp_tls_policy_maps = hash:/etc/postfix/tls_policy
```

```
# /etc/postfix/tls_policy
mailrepo.de    encrypt
```

```
postmap /etc/postfix/tls_policy && systemctl reload postfix
```

53 Microsoft 365 / Exchange Online

1. Öffnen Sie das **Exchange Admin Center** → **Nachrichtenfluss** → **Regeln**.
2. Klicken Sie auf **Regel hinzufügen** → **Neue Regel erstellen**.
3. **Name:** z. B. „Archivierung mailrepo.de"
4. **Bedingung:** *Absender ist intern* (für ausgehende) oder *Empfänger ist intern* (für eingehende) — oder beides.
5. **Aktion:** *BCC an* → `archive-vautron-100123@mailrepo.de`
6. Speichern und aktivieren.

Für getrennte Tags können Sie zwei Regeln anlegen — eine für eingehend, eine für ausgehend.

TLS erzwingen: Erstellen Sie unter **Nachrichtenfluss → Connectors** einen Partner-Connector zu mailrepo.de mit der Option *TLS erzwingen und gültiges Zertifikat verlangen*.

54 Google Workspace

1. Öffnen Sie die **Google Admin Console** → **Apps** → **Google Workspace** → **Gmail** → **Routing**.

2. Klicken Sie auf **Regel hinzufügen**.
3. **Betroffene Nachrichten:** Eingehend, Ausgehend, Intern (nach Bedarf).
4. **Empfänger hinzufügen:** `archive-vautron-100123@mailrepo.de`
5. **Zustellungsoption:** *BCC hinzufügen*
6. Speichern.

   TLS erzwingen: Aktivieren Sie unter **Compliance → TLS-Konformität** eine Regel für die Domain `mailrepo.de` mit *TLS-Verbindung erforderlich*.

55 Andere Mailserver

Mailserver	Konfiguration
Exim	Über einen Router vom Typ `redirect` mit `unseen`
Sendmail	`.mc`-Konfiguration mit `FEATURE(always_bcc)`
Dovecot + Sieve	`redirect`-Aktion in einem globalen Sieve-Script
Zimbra	Admin-Konsole → Postfix-Einstellungen → `always_bcc`
MDaemon	Sicherheit → Inhaltsfilter → BCC-Regel
Kerio Connect	Zustellungsregeln → Kopie weiterleiten

Bei Fragen zur Konfiguration wenden Sie sich an den Support.

56 Archiv nutzen

Nach der Einrichtung werden Mails automatisch archiviert. Im Dashboard sehen Sie den aktuellen Stand. Über die Suche finden Sie archivierte Mails — die Entschlüsselung erfolgt bei Bedarf direkt im Browser.

---

57 Häufige Fragen (FAQ)

Kann der Betreiber meine E-Mails lesen?
Nein. Die Entschlüsselung findet ausschließlich in Ihrem Browser statt. Der Server speichert nur verschlüsselte Daten.

Was passiert, wenn ich mein Passwort vergesse?
Sie können den Zugang mit Ihrer 12-Wort-Wiederherstellungsphrase zurücksetzen. Ohne Passwort und ohne Phrase ist eine Entschlüsselung nicht möglich — auch nicht durch den Betreiber. Falls HSM-Escrow aktiviert ist, kann der Betreiber eine betreute Wiederherstellung durchführen: Ihr privater Schlüssel wird sicher auf dem HSM entschlüsselt, neu gewrapped und Ihnen wird eine neue Wiederherstellungsphrase zugestellt.

Wie lange werden meine Mails aufbewahrt?
Die Aufbewahrungsdauer richtet sich nach Ihrem Vertrag und den gesetzlichen Vorgaben (z. B. GoBD: bis zu 10 Jahre).

Kann ich einzelne Mails löschen?
Ja, über die Detailansicht im Web-Portal. Löschungen werden protokolliert und in der Audit-Kette vermerkt.

Wie finde ich eine bestimmte Mail?
Die semantische Suche versteht Synonyme und verwandte Begriffe. Beschreiben Sie einfach, wonach Sie suchen — auch wenn Sie die genauen Worte nicht kennen.

Was beweist die Audit-Kette?
Die Audit-Kette beweist, wann welche Mail archiviert wurde und dass die Reihenfolge nicht verändert wurde. Jeder Eintrag ist von einer unabhängigen Zeitstempelstelle bestätigt.

Ist das System gegen Quantencomputer geschützt?
Die Audit-Kette unterstützt bereits ML-DSA-65, einen post-quanten-sicheren Algorithmus. Für die Mail-Verschlüsselung (RSA-4096) bietet die Zero-Knowledge-Architektur zusätzlichen Schutz: Da der Server niemals den Klartext sieht, müsste ein Angreifer Ihren privaten Schlüssel direkt angreifen.

Wo werden meine Daten gespeichert?
Alle Daten werden in einem deutschen Rechenzentrum gespeichert. Es findet keine Übertragung ins Ausland statt. Der Speicher nutzt dreifache Replikation für maximale Ausfallsicherheit.

---

58 Glossar

Begriff	Erklärung
AES-256-GCM	Symmetrischer Verschlüsselungsalgorithmus mit 256-Bit-Schlüssel und authentifizierter Verschlüsselung.
Argon2id	Passwort-Hashing-Algorithmus, speziell gegen Brute-Force-Angriffe mit Spezialhardware geschützt.
BIP-39	Standard für mnemonische Wiederherstellungsphrasen (12 Wörter).
DEK	Data Encryption Key — zufälliger Schlüssel, der pro Mail erzeugt wird.
DSGVO	Datenschutz-Grundverordnung der EU.
Ed25519	Digitales Signaturverfahren auf Basis elliptischer Kurven.
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern und Aufzeichnungen in elektronischer Form.
HKDF	HMAC-based Key Derivation Function — leitet aus einem Master-Secret deterministisch Schlüssel ab.
HSM	Hardware Security Module — spezialisierte Hardware zur sicheren Schlüsselspeicherung.
KEK	Key Encryption Key — Schlüssel, der andere Schlüssel verschlüsselt.
Merkle-Baum	Binäre Hash-Struktur, die viele Einträge in einem Root-Hash zusammenfasst.
ML-DSA-65	Post-quanten-sicherer Signaturalgorithmus (ehemals CRYSTALS-Dilithium).
OAEP	Optimal Asymmetric Encryption Padding — Padding-Schema für RSA-Verschlüsselung.

Begriff	Erklärung
PBKDF2	Password-Based Key Derivation Function 2 — leitet aus einem Passwort einen kryptographischen Schlüssel ab.
RFC 3161	Standard für vertrauenswürdige Zeitstempeldienste (TSA).
RSA-4096	Asymmetrisches Verschlüsselungsverfahren mit 4096-Bit-Schlüsseln.
TOTP	Time-based One-Time Password — zeitbasiertes Einmalpasswort zur Zwei-Faktor-Authentifizierung.
TSA	Timestamp Authority — unabhängige Zeitstempelstelle.
WebAuthn / Passkey	Web-Authentication-Standard (W3C/FIDO2) — ermöglicht die Anmeldung per Fingerabdruck, Face ID oder USB-Sicherheitsschlüssel statt eines TOTP-Codes.
WebCrypto API	Browser-native Kryptographie-Schnittstelle nach W3C-Standard.
Zero-Knowledge	Architekturprinzip, bei dem der Server keine Kenntnis der unverschlüsselten Daten hat.

Dieses Handbuch beschreibt die Nutzung und Sicherheit des mailrepo.de-Archivierungssystems aus Kundensicht.