VAUTRON
RECHENZENTRUM AG

# mailrepo.de — Security Whitepaper

April 2026 · Version 1.0

Vautron Rechenzentrum AG

## Inhaltsverzeichnis

# 1 Zusammenfassung

mailrepo.de ist ein E-Mail-Archivierungsdienst der Vautron Rechenzentrum AG. Dieses Whitepaper beschreibt die Sicherheitsarchitektur für IT-Entscheider, Datenschutzbeauftragte und Auditoren.

Die zentralen Sicherheitseigenschaften:

- **Zero-Knowledge-Architektur** — Im vorgesehenen Sicherheitsmodell hat der Betreiber zu keinem Zeitpunkt Zugriff auf E-Mail-Klartext.*
- **Ende-zu-Ende-Verschlüsselung** — Verschlüsselung und Entschlüsselung finden ausschließlich im Browser des Nutzers statt.
- **Kryptographische Audit-Kette** — Jede archivierte E-Mail wird in einer manipulationssicheren, signierten und zeitgestempelten Hash-Kette protokolliert.
- **Post-Quantum-Vorbereitung** — Die Architektur ist algorithmen-agil und für den Einsatz post-quantensicherer Verfahren vorbereitet.
- **Deutsches Rechenzentrum** — ISO/IEC 27001-zertifiziert, keine Drittland-Übertragung.

* *Bei aktiviertem HSM-Escrow-Dienst kann der Mandanten-Administrator unter Einsatz des physischen Hardware-Security-Moduls eine Wiederherstellung durchführen. Siehe Abschnitt „HSM-Escrow“.*

# 2 Verschlüsselungsarchitektur

## 2.1 Schlüsselhierarchie

Die Verschlüsselung basiert auf einer 5-stufigen Schlüsselhierarchie. Der Dienst speichert zu keinem Zeitpunkt den privaten Schlüssel eines Kunden im Klartext.

| Ebene | Algorithmus | Parameter |
|---|---|---|
| Mail-Inhalt | AES-256-GCM | 256-Bit Key, 12-Byte IV, 16-Byte AuthTag |
| DEK-Wrapping | RSA-OAEP-SHA256 | 4096-Bit RSA |
| Privater Schlüssel | AES-GCM Key Wrap | 256-Bit KEK, 12-Byte IV |
| KEK aus Passwort | PBKDF2-SHA-256 | 600.000 Iterationen, 32-Byte Salt |
| KEK aus Recovery | HKDF-SHA-256 | Deterministisch aus BIP-39 Seed |

**Ablauf:** Für jede E-Mail wird ein zufälliger Data Encryption Key (DEK) generiert. Der DEK verschlüsselt den Mail-Inhalt mit AES-256-GCM. Der DEK selbst wird mit dem öffentlichen RSA-4096-Schlüssel des Kunden verschlüsselt (RSA-OAEP). Der private Schlüssel existiert nur im Browser, geschützt durch ein passwortbasiertes KEK. Nach der Verschlüsselung wird der DEK im Arbeitsspeicher sofort mit Nullbytes überschrieben.

## 2.2 Zero-Knowledge-Prinzip

Der Server verarbeitet E-Mails nur in verschlüsselter Form. Die Entschlüsselung findet ausschließlich über die WebCrypto API im Browser statt. Private Schlüssel werden als `non-extractable` CryptoKey-Objekte gehalten.

Der Auth-Hash-Salt ist kryptographisch vom KEK-Salt getrennt — die Kenntnis des Authentifizierungs-Hashes ermöglicht keinen Rückschluss auf den Verschlüsselungsschlüssel.

**Hinweis:** Bei aktiviertem HSM-Escrow-Dienst (siehe unten) kann der Mandanten-Administrator unter Einsatz des physischen Hardware-Security-Moduls den privaten Schlüssel eines Benutzers wiederherstellen. Das Zero-Knowledge-Prinzip gilt in diesem Fall eingeschränkt.

## 2.3 Schlüsselwiederherstellung

Jeder Benutzer erhält bei der Registrierung eine 12-Wort-Wiederherstellungsphrase (BIP-39). Diese ermöglicht die Wiederherstellung des privaten Schlüssels unabhängig vom Passwort:

Mnemonic → PBKDF2-SHA-512 (2.048 Iterationen) → 512-Bit Seed → HKDF-SHA-256 → Recovery-KEK → AES-GCM Unwrap des privaten Schlüssels.

## 2.4 HSM-Escrow (optional)

Für Unternehmen, die eine administrative Wiederherstellung benötigen, steht ein Hardware-Security-Module-basiertes Escrow-Verfahren zur Verfügung:

- Nitrokey SmartCard-HSM (Nitrokey HSM2)
- RSA-4096 Escrow-Schlüssel, nicht exportierbar
- Hybrid-Verschlüsselung: AES-256-GCM + RSA-OAEP-SHA256
- Entschlüsselung nur mit physischem HSM-Zugriff und PIN (PKCS#11)

Das Escrow-Verfahren ist optional und erfordert die explizite Aktivierung durch den Mandanten-Administrator.

# 3 Authentifizierung

| Maßnahme | Detail |
|---|---|
| Passwort-Policy | Erzwungene Komplexitätsanforderungen (Länge, Zeichenklassen) |
| Client-side Hashing | PBKDF2-SHA-256 |
| Server-side Hashing | Argon2id |
| Zwei-Faktor | TOTP (RFC 6238) und/oder FIDO2/WebAuthn (Passkeys) |
| Backup-Codes | Einmalcodes, gehashed, Constant-Time-Verifikation |
| Kontosperre | Automatische Sperre nach wiederholten Fehlversuchen |
| Sessions | Sichere Cookie-Flags, IP-Binding, automatischer Ablauf bei Inaktivität |

TOTP-Secrets werden auf dem Server verschlüsselt gespeichert. WebAuthn unterstützt aktuelle Algorithmen mit Clone-Detection.

# 4 Audit-Kette (Ledger)

## 4.1 Aufbau

Jede archivierte E-Mail, jede Löschung und jede administrative Aktion wird in einer kryptographischen Hash-Kette (Ledger) protokolliert. Die Kette ist append-only und besteht aus vier Ebenen:

| Ebene | Scope | Signiert | Zeitgestempelt |
|---|---|---|---|
| Events | Pro Kunde | — | — |
| Commits | Pro Kunde | Ja | Ja (RFC 3161) |
| Tenant Heads | Pro Mandant | Ja | Ja |
| Root Heads | Global | Ja | Ja |

Events werden in Commits zusammengefasst, deren Integrität durch einen Merkle-Baum (RFC 6962) gesichert wird. Domain Separation verhindert Second-Preimage-Angriffe.

## 4.2 Signaturalgorithmen

Der Ledger ist algorithmen-agil — mehrere Signaturverfahren können parallel in derselben Kette koexistieren:

| Algorithmus | Standard | Sicherheitsniveau |
|---|---|---|
| Ed25519 | RFC 8032 | 128 Bit |
| ECDSA P-256 | FIPS 186-5 | 128 Bit |
| ECDSA brainpoolP256r1 | RFC 5639, BSI TR-03111 | 128 Bit |
| ML-DSA-65 | FIPS 204 (Post-Quantum) | NIST Level 3 |

Die Schlüsselrotation erfolgt über eine API (`rotate-key`) — neue Schlüssel werden automatisch generiert, der aktive Schlüssel atomar umgeschaltet. Alte Schlüssel bleiben zur Verifikation verfügbar.

### 4.3 Zeitstempel (TSA)

Commits werden mit qualifizierten Zeitstempeln nach RFC 3161 versehen. Die Zeitstempel stammen von unabhängigen Timestamping Authorities und bieten Non-Repudiation — auch wenn zukünftige Quantencomputer klassische Signaturen brechen sollten.

Unterstützte Hash-Algorithmen: SHA-256, SHA-512, SHA3-256. Im `fail_closed`-Modus wird ein Commit ohne erfolgreichen Zeitstempel abgelehnt.

### 4.4 Proof Bundles

Für jede archivierte E-Mail kann ein Merkle Inclusion Proof exportiert werden. Dieser enthält den Hash des Eintrags, die Geschwister-Hashes des Merkle-Pfades, die Signatur des Commits und den TSA-Zeitstempel. Proof Bundles sind offline verifizierbar und enthalten ausschließlich Daten des eigenen Mandanten.

## 5 Post-Quantum-Vorbereitung

Die eingesetzten symmetrischen Verfahren (AES-256-GCM, SHA-256/512, SHA3-256) gelten als quantensicher. Für asymmetrische Verfahren (Ed25519, ECDSA, RSA) besteht ein langfristiges Risiko durch Quantencomputer (Shor-Algorithmus).

Die Architektur ist darauf vorbereitet:

- **Algorithmen-Agilität:** Die Audit-Kette unterstützt mehrere Signaturverfahren parallel. Post-quantensichere Algorithmen (z. B. ML-DSA-65, FIPS 204) können ohne Unterbrechung bestehender Ketten eingeführt werden.
- **TSA-Absicherung:** Unabhängige RFC-3161-Zeitstempel bieten zusätzliche Non-Repudiation für historische Signaturen.
- **Schrittweise Migration:** Bei Verfügbarkeit entsprechender Browser-Standards (WebCrypto) ist eine Migration der E-Mail-Verschlüsselung auf post-quantensichere Verfahren vorgesehen.

## 6 Mandantentrennung

### 6.1 Datenebene

Sämtliche Abfragen sind mandantengetrennt. Cross-Tenant-Zugriffe sind durch das Sicherheitsmodell ausgeschlossen.

### 6.2 Schlüsselebene

Jeder Benutzer besitzt ein eigenes RSA-4096-Schlüsselpaar. Schlüssel sind an die Kombination aus Mandant und Kundennummer gebunden.

### 6.3 Speicherebene

Verschlüsselte E-Mails werden unter mandantenspezifischen Pfaden abgelegt. Jeder Mandant hat einen dedizierten Speicherbereich.

### 6.4 Audit-Kette

Der Ledger führt separate Event-Chains pro Mandant und Kunde. Tenant Heads aggregieren die Integrität auf Mandantenebene. Proof Bundles enthalten ausschließlich Daten des eigenen Mandanten.

### 6.5 Berechtigungskonzept

Der Zugriff auf die Infrastruktur ist über ein abgestuftes Rollenkonzept nach dem Prinzip der minimalen Rechte (Principle of Least Privilege) geregelt.

## 7 Betreiberzugriffe

**Im vorgesehenen Sicherheitsmodell hat Vautron keinen Zugriff auf E-Mail-Klartext.** Der private Schlüssel jedes Kunden existiert nur in verschlüsselter Form auf dem Server. Die Entschlüsselung erfordert das Passwort oder die Wiederherstellungsphrase des Kunden — beides ist dem Betreiber nicht bekannt.

Administrativer Zugriff auf die Infrastruktur erfolgt ausschließlich über ein zentrales SSH-Gateway mit Zwei-Faktor-Authentifizierung. Alle Zugriffe werden protokolliert.

Das optionale HSM-Escrow-Verfahren erfordert physischen Zugang zum Hardware-Security-Module und dessen PIN. Es wird nur auf explizite Anforderung des Mandanten aktiviert.

## 8 Netzwerk und Härtung

Alle Dienste laufen mit eingeschränkten Betriebssystem-Policies nach dem Prinzip der minimalen Rechte. Die wichtigsten Maßnahmen:

- **Transportverschlüsselung:** Sämtliche Kommunikation erfolgt über TLS (ab Version 1.2). Das Web-Portal erzwingt HTTPS mit HSTS Preload.
- **Security Headers:** Content-Security-Policy, HSTS, Frame-Schutz und Referrer-Policy sind konfiguriert. Externe Skripte und CDNs werden nicht eingesetzt.
- **Sandboxing:** E-Mail-Inhalte werden in einer isolierten Umgebung ohne Skript-Ausführung gerendert.
- **Rate Limiting:** Alle Endpunkte sind gegen Brute-Force- und Denial-of-Service-Angriffe geschützt. Token-Vergleiche erfolgen in konstanter Zeit.
- **Netzwerksegmentierung:** Dienste kommunizieren ausschließlich über authentifizierte interne Schnittstellen.

## 9 Speicherung und Verfügbarkeit

### 9.1 Objektspeicher

- Mehrfache Replikation auf unabhängigen Knoten
- Self-Healing bei Knotenausfall
- Checksummen auf Blockebene (Bit-Rot-Erkennung)

### 9.2 Datenbank

- Tägliche Backups mit Point-in-Time-Recovery

### 9.3 Ledger

- Append-only Journals mit Frame-Checksummen
- Index jederzeit aus Journals rebuildfähig
- Snapshots und Export über API

### 9.4 Standort

Alle Daten werden ausschließlich in deutschen Rechenzentren der Vautron Rechenzentrum AG verarbeitet und gespeichert. Es findet keine Übermittlung in Drittländer statt.

## 10 Suche — Datenschutz durch Design

### 10.1 Vektorbasierte Suche

Der Suchindex speichert keine Klartexte. E-Mail-Inhalte werden lokal in 768-dimensionale Vektoren transformiert (KI-Modell läuft ausschließlich im Rechenzentrum). Eine Rekonstruktion des Originaltexts aus den Vektoren ist nach aktuellem Stand der Technik nicht möglich.

### 10.2 DSGVO-Bereinigung vor Indexierung

Vor der Vektorisierung werden personenbezogene Daten automatisch entfernt:

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

Ein 3-Hash-Audit-Trail dokumentiert jeden Bereinigungsschritt: Original-Hash → Bereinigt-Hash → Redaktiert-Hash.

## 11 Incident Response

### 11.1 Kontokompromittierung

1. Sofortige Kontosperre
2. TOTP-Secret-Rotation
3. Backup-Code-Regenerierung
4. Login-Historie-Analyse
5. Session-Terminierung

### 11.2 Schlüsselkompromittierung (Ledger)

1. Sofortige Schlüsselrotation
2. Neue Commits verwenden den neuen Schlüssel
3. TSA-Zeitstempel auf bestehenden Commits bieten unabhängige Verifikation

### 11.3 Manipulationsverdacht

Automatisierte Kettenverifikation (`verify-chain`) mit TSA-Timestamp-Prüfung. Integritätsverletzungen werden sofort gemeldet.

## 12 Kontakt

**Vautron Rechenzentrum AG**
Obermünsterstraße 9
93047 Regensburg
Deutschland

**Datenschutzbeauftragter:** datenschutz@vautron.de
**Technischer Support:** server@vautron.de