VAUTRON
RECHENZENTRUM AG

mailrepo.de — Security Whitepaper

April 2026 · Version 1.0

Vautron Rechenzentrum AG

Contents

1 Executive Summary

mailrepo.de is an email archiving service operated by Vautron Rechenzentrum AG. This whitepaper describes the security architecture for IT decision-makers, data protection officers and auditors.

Core security properties:

- **Zero-Knowledge Architecture** — Under the designed security model, the operator never has access to email plaintext.*
- **End-to-End Encryption** — Encryption and decryption take place exclusively in the user's browser.
- **Cryptographic Audit Chain** — Every archived email is logged in a tamper-proof, signed and timestamped hash chain.
- **Post-Quantum Preparation** — The architecture is algorithm-agile and prepared for the adoption of post-quantum secure algorithms.
- **German Data Center** — ISO/IEC 27001-certified, no third-country transfers.

* *When the HSM escrow service is enabled, the tenant administrator can perform key recovery using the physical Hardware Security Module. See section "HSM Escrow".*

2 Encryption Architecture

2.1 Key Hierarchy

Encryption is based on a 5-level key hierarchy. The service never stores a customer's private key in plaintext.

Level	Algorithm	Parameters
Mail content	AES-256-GCM	256-bit key, 12-byte IV, 16-byte AuthTag
DEK wrapping	RSA-OAEP-SHA256	4096-bit RSA
Private key	AES-GCM Key Wrap	256-bit KEK, 12-byte IV

Level	Algorithm	Parameters
KEK from password	PBKDF2-SHA-256	600,000 iterations, 32-byte salt
KEK from recovery	HKDF-SHA-256	Deterministic from BIP-39 seed

Flow: For each email, a random Data Encryption Key (DEK) is generated. The DEK encrypts the email content with AES-256-GCM. The DEK itself is encrypted with the customer's RSA-4096 public key (RSA-OAEP). The private key exists only in the browser, protected by a password-derived KEK. After encryption, the DEK is immediately zeroed in memory.

2.2 Zero-Knowledge Principle

The server processes emails only in encrypted form. Decryption takes place exclusively via the WebCrypto API in the browser. Private keys are held as `non-extractable` CryptoKey objects.

The auth hash salt is cryptographically separated from the KEK salt — knowledge of the authentication hash does not reveal the encryption key.

Note: When the HSM escrow service is enabled (see below), the tenant administrator can recover a user's private key using the physical Hardware Security Module. The zero-knowledge principle is limited in this case.

2.3 Key Recovery

Each user receives a 12-word recovery phrase (BIP-39) during registration. This enables private key recovery independent of the password:

Mnemonic → PBKDF2-SHA-512 (2,048 iterations) → 512-bit seed → HKDF-SHA-256 → Recovery KEK → AES-GCM unwrap of private key.

2.4 HSM Escrow (Optional)

For enterprises requiring administrative key recovery, a Hardware Security Module-based escrow procedure is available:

- Nitrokey SmartCard-HSM (Nitrokey HSM2)
- RSA-4096 escrow key, non-exportable
- Hybrid encryption: AES-256-GCM + RSA-OAEP-SHA256
- Decryption only with physical HSM access and PIN (PKCS#11)

The escrow procedure is optional and requires explicit activation by the tenant administrator.

3 Authentication

Measure	Detail
Password policy	Enforced complexity requirements (length, character classes)
Client-side hashing	PBKDF2-SHA-256
Server-side hashing	Argon2id

Measure	Detail
Two-factor	TOTP (RFC 6238) and/or FIDO2/WebAuthn (Passkeys)
Backup codes	One-time codes, hashed, constant-time verification
Account lockout	Automatic lockout after repeated failed attempts
Sessions	Secure cookie flags, IP binding, automatic expiry on inactivity

TOTP secrets are stored encrypted on the server. WebAuthn supports current algorithms with clone detection.

4 Audit Chain (Ledger)

4.1 Structure

Every archived email, every deletion and every administrative action is logged in a cryptographic hash chain (Ledger). The chain is append-only and consists of four levels:

Level	Scope	Signed	Timestamped
Events	Per customer	—	—
Commits	Per customer	Yes	Yes (RFC 3161)
Tenant Heads	Per tenant	Yes	Yes
Root Heads	Global	Yes	Yes

Events are aggregated into commits whose integrity is secured by a Merkle tree (RFC 6962). Domain separation prevents second-preimage attacks.

4.2 Signature Algorithms

The Ledger is algorithm-agile — multiple signature schemes can coexist in the same chain:

Algorithm	Standard	Security Level
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

Key rotation is performed via API (`rotate-key`) — new keys are generated automatically, the active key is switched atomically. Previous keys remain available for verification.

4.3 Timestamps (TSA)

Commits are signed with qualified timestamps per RFC 3161. Timestamps originate from independent Timestamping Authorities and provide non-repudiation — even if future quantum computers break classical signatures.

Supported hash algorithms: SHA-256, SHA-512, SHA3-256. In `fail_closed` mode, a commit without a successful timestamp is rejected.

4.4 Proof Bundles

For every archived email, a Merkle inclusion proof can be exported. It contains the entry hash, sibling hashes of the Merkle path, the commit signature and the TSA timestamp. Proof bundles are verifiable offline and contain exclusively data from the requesting tenant.

5 Post-Quantum Preparation

The symmetric algorithms in use (AES-256-GCM, SHA-256/512, SHA3-256) are considered quantum-safe. Asymmetric algorithms (Ed25519, ECDSA, RSA) face a long-term risk from quantum computers (Shor's algorithm).

The architecture is prepared for this:

- **Algorithm Agility:** The audit chain supports multiple signature schemes in parallel. Post-quantum secure algorithms (e.g. ML-DSA-65, FIPS 204) can be introduced without disrupting existing chains.
- **TSA Assurance:** Independent RFC 3161 timestamps provide additional non-repudiation for historical signatures.
- **Stepwise Migration:** Migration of email encryption to post-quantum secure algorithms is planned once corresponding browser standards (WebCrypto) become available.

6 Tenant Isolation

6.1 Data Level

All queries are tenant-scoped. Cross-tenant access is prevented by the security model.

6.2 Key Level

Every user has their own RSA-4096 key pair. Keys are bound to the combination of tenant and customer number.

6.3 Storage Level

Encrypted emails are stored under tenant-specific paths. Each tenant has a dedicated storage area.

6.4 Audit Chain

The Ledger maintains separate event chains per tenant and customer. Tenant Heads aggregate integrity at the tenant level. Proof bundles contain exclusively data from the requesting tenant.

6.5 Authorization Concept

Infrastructure access is governed by a tiered role concept following the Principle of Least Privilege.

7 Operator Access

Under the designed security model, Vautron has no access to email plaintext. Each customer's private key exists only in encrypted form on the server. Decryption requires the customer's password or recovery phrase — neither of which is known to the operator.

Administrative infrastructure access is exclusively through a central SSH gateway with two-factor authentication. All access is logged.

The optional HSM escrow procedure requires physical access to the Hardware Security Module and its PIN. It is only activated upon explicit request from the tenant.

8 Network and Hardening

All services run with restricted operating system policies following the Principle of Least Privilege. Key measures:

- **Transport Encryption:** All communication uses TLS (version 1.2 or higher). The web portal enforces HTTPS with HSTS preload.
- **Security Headers:** Content-Security-Policy, HSTS, frame protection and referrer policy are configured. No external scripts or CDNs are used.
- **Sandboxing:** Email content is rendered in an isolated environment without script execution.
- **Rate Limiting:** All endpoints are protected against brute-force and denial-of-service attacks. Token comparisons use constant-time operations.
- **Network Segmentation:** Services communicate exclusively through authenticated internal interfaces.

9 Storage and Availability

9.1 Object Storage

- Multiple replication across independent nodes
- Self-healing on node failure
- Block-level checksums (bit-rot detection)

9.2 Database

- Daily backups with point-in-time recovery

9.3 Ledger

- Append-only journals with frame checksums
- Index rebuildable from journals at any time

- Snapshots and export via API

9.4 Location

All data is exclusively processed and stored in German data centers operated by Vautron Rechenzentrum AG. No transfer to third countries takes place.

10 Search — Privacy by Design

10.1 Vector-Based Search

The search index stores no plaintext. Email content is transformed locally into 768-dimensional vectors (AI model runs exclusively in the data center). Reconstruction of the original text from the vectors is not possible according to the current state of the art.

10.2 GDPR Redaction Before Indexing

Before vectorization, personal data is automatically removed:

1. Passwords and credentials
2. API keys and tokens
3. IBANs and bank details
4. Phone numbers
5. Postal addresses
6. Email addresses
7. Customer numbers

A 3-hash audit trail documents each redaction step: original hash → cleaned hash → redacted hash.

11 Incident Response

11.1 Account Compromise

1. Immediate account lockout
2. TOTP secret rotation
3. Backup code regeneration
4. Login history analysis
5. Session termination

11.2 Key Compromise (Ledger)

1. Immediate key rotation
2. New commits use the new key
3. TSA timestamps on existing commits provide independent verification

11.3 Suspected Tampering

Automated chain verification (`verify-chain`) with TSA timestamp checking. Integrity violations are reported immediately.

12 Contact

Vautron Rechenzentrum AG
Obermünsterstraße 9
93047 Regensburg
Germany

Data Protection Officer: datenschutz@vautron.de
Technical Support: server@vautron.de