

Key Management Policy

Key Management Policy

“ **Organization:** Bilko — Balkan Accounting SaaS **Policy Number:** POL-SEC-KM-001 **Version:** 1.0 **Date:** 2026-02-23 **Author:** CTO **Status:** Draft **Reviewers:** DPO, Engineering Lead **Classification:** Confidential — Restricted

Document History

Version	Date	Author	Changes
0.1	2026-02-23	CTO	Initial key management policy for Bilko

1. Purpose & Scope

This policy defines the lifecycle management for all cryptographic keys and secrets used by Bilko. It covers key generation, storage, rotation, revocation, and destruction.

Scope: All Bilko production and staging environments. All personnel with access to Railway environment variables or Vaultwarden.

2. Key Inventory

Key ID	Key Type	Purpose	Storage	Rotation Period	Owner
JWT_PRIVATE_KEY	RSA 2048-bit private key	JWT access token signing (RS256)	Railway secret (production)	Annual	CTO
JWT_PUBLIC_KEY	RSA 2048-bit public key	JWT access token verification	Railway secret (production)	Annual (with private)	CTO

Key ID	Key Type	Purpose	Storage	Rotation Period	Owner
REFRESH_TOKEN_SECRET	64-byte random hex	Refresh token HMAC signing	Railway secret	Annual	CTO
FIELD_ENCRYPTION_KEY	32-byte random hex (AES-256)	Field-level encryption of PIB/JMBG/OIB/JIB/IBAN	Railway secret	Annual	CTO
FIELD_HMAC_KEY	32-byte random hex	Deterministic HMAC for searchable hash on encrypted fields	Railway secret	Annual (with FIELD_ENCRYPTION_KEY)	CTO
DATABASE_URL	PostgreSQL connection string with credentials	Database access	Railway secret	On compromise / quarterly review	CTO
SEF_API_KEY	API key string	Serbia SEF e-invoice portal (per org)	DB (encrypted) per org	Per SEF portal policy	Per organization
FINA_CERT	X.509 certificate + private key	HR-FISK e-invoice signing (FINA PKI)	DB (encrypted) per org	Per FINA PKI (1-3 years)	Per organization
SENTRY_DSN	DSN string	Error tracking	Railway secret / env var	On compromise	CTO

3. Key Hierarchy

```
graph TD
  ROOT["Root Secrets\n(CTO personal Vaultwarden vault)"]
  RAILWAY["Railway Environment Secrets\n(production / staging / dev)"]
  ORG_SECRETS["Per-Organization Secrets\n(DB encrypted, L4 Restricted)\nSEF API keys, FINA certs"]
  APP["Application Runtime\n(keys loaded from env at startup)"]

  ROOT -->|"Provision"| RAILWAY
  RAILWAY -->|"Load at boot"| APP
  ROOT -->|"Rotation authority"| ORG_SECRETS
  ORG_SECRETS -->|"Decrypt on request"| APP
```

Principle: No key material is ever committed to source code. No key is stored in plaintext outside Railway secrets or Vaultwarden.

4. Key Generation Standards

Key Type	Generation Method	Entropy Requirements
RSA (JWT)	<code>openssl genrsa 2048</code>	2048-bit minimum
Symmetric (AES-256)	<code>openssl rand -hex 32</code>	256 bits (32 bytes)
HMAC key	<code>openssl rand -hex 32</code>	256 bits
Refresh token secret	<code>openssl rand -hex 64</code>	512 bits
API keys (external)	Generated by external portal (SEF/FINA)	Per external system

Commands:

```
# Generate JWT key pair
openssl genrsa -out jwt_private.pem 2048
openssl rsa -in jwt_private.pem -pubout -out jwt_public.pem

# Generate AES-256 field encryption key
openssl rand -hex 32

# Generate HMAC key
openssl rand -hex 32
```

All generated keys must be imported to Railway and Vaultwarden within 1 hour. Local files deleted securely after import.

5. Key Storage

Production Keys (Railway)

- All production keys stored as Railway environment variables
- Railway EU West region — encrypted at rest by Railway (AES-256)
- Access: CTO + one designated backup (CEO) only
- Two-factor authentication mandatory for Railway account
- Railway account uses ALAI SSO / strong password (≥20 chars, in Vaultwarden)

Staging/Dev Keys

- Separate Railway project (staging) — different keys from production
- Dev: `.env.local` files excluded from git via `.gitignore`
- Dev keys may use weaker entropy but must still be valid format

Vaultwarden (Backup & Documentation)

- URL: <https://vault.basicconsulting.no>
- Stores: production key material as secure notes (encrypted)
- Access: CTO + CEO (break-glass access)
- Purpose: Recovery if Railway secrets are lost; rotation documentation

Per-Organization Secrets (SEF API Keys, FINA Certificates)

- Stored in PostgreSQL `OrganizationSecret` table
- Value encrypted with `FIELD_ENCRYPTION_KEY` before storage
- Decrypted in-memory only when needed for API call
- FINA private keys additionally protected with password (stored separately)

6. Key Rotation Procedures

6.1 Annual Rotation (Standard)

Schedule: First Monday of each calendar year.

FIELD_ENCRYPTION_KEY rotation (most sensitive — requires re-encryption):

1. Generate new `FIELD_ENCRYPTION_KEY` (`openssl rand -hex 32`)
2. Deploy a migration job that:
 - a. Reads each encrypted field with old key
 - b. Decrypts
 - c. Re-encrypts with new key
 - d. Writes back to DB
3. Migration must be atomic per record (read old → write new in transaction)
4. Only after 100% migration: update Railway secret to new key
5. Delete old key from Vaultwarden (add to archive note with date)
6. Test: attempt decryption with both old (should fail) and new (should succeed) keys

JWT key pair rotation (zero-downtime):

1. Generate new RSA key pair
2. Add new public key to JWKS endpoint alongside old (support both during rotation window)
3. Begin issuing new tokens signed with new private key
4. Wait for all old tokens to expire (15 minutes max)
5. Remove old public key from JWKS
6. Update JWT_PRIVATE_KEY and JWT_PUBLIC_KEY in Railway
7. Invalidate all refresh tokens (users will re-login)

6.2 Emergency Rotation (On Compromise)

If a key is suspected compromised:

1. **Immediately** invalidate: all user sessions (clear RefreshToken table)
2. Generate new key within 15 minutes
3. Update Railway secret
4. Deploy new application instance (Railway auto-deploys on env var change)
5. Document in Vaultwarden: old key, date of compromise, date of rotation
6. Assess whether breach notification is required (see data-breach-response-plan.md)

6.3 FINA Certificate (HR-FISK) Rotation

FINA X.509 certificates for HR-FISK e-invoicing have a defined validity period (1-3 years per FINA PKI).

1. FINA certificate expiry alert fires 60 days before expiry
2. Organization admin is notified to renew via FINA portal
3. New certificate uploaded through Bilko settings → HR eRačun → Certificate
4. Old certificate archived (not deleted – needed to verify past submissions)
5. Test: submit a test e-invoice via HR-FISK test environment with new certificate

7. Key Access Control

Key	Who Can Access	How
JWT_PRIVATE_KEY	Application only (Railway env)	Never exposed via API; loaded at startup
FIELD_ENCRYPTION_KEY	Application only	Never logged; never returned in API response
DATABASE_URL	Application + CTO	Railway secret; CTO can view in Railway dashboard

Key	Who Can Access	How
SEF API keys	Application + org owner	Decrypted only for SEF API calls; org owner can rotate via settings
FINA certificates	Application + org owner	Decrypted only for HR-FISK submissions

Access log: All Railway secret views logged in Railway audit trail. Any access outside normal deployment is reviewed by CTO.

8. Escrow & Recovery

FIELD_ENCRYPTION_KEY Escrow (Critical)

The FIELD_ENCRYPTION_KEY is the most critical key — loss means permanent loss of all L4 Restricted field data (tax IDs, IBAN).

Escrow procedure:

- FIELD_ENCRYPTION_KEY stored in Vaultwarden secure note accessible to: CTO, CEO
- Vaultwarden has its own backup (see system infrastructure docs)
- Key material noted with: creation date, rotation date, description

If FIELD_ENCRYPTION_KEY is lost and not recoverable: All encrypted field data is permanently unreadable. This is a catastrophic data loss event. Contact legal counsel and affected supervisory authorities.

Railway Account Recovery

- Railway root account: admin@bilko.io (password in Vaultwarden)
 - 2FA recovery codes: Vaultwarden secure note
 - Designated backup access: CEO has view access to Railway (read-only)
-

9. Key Destruction

When a key is retired (superseded by rotation):

1. Remove from Railway environment variables
2. Remove from active Vaultwarden entries
3. Archive to Vaultwarden secure note: "Retired Keys" with date and reason

4. Old FIELD_ENCRYPTION_KEY versions: retained for 3 months after rotation (in case rollback needed), then permanently deleted from Vaultwarden
-

Approval

Role	Name	Signature	Date
Author	CTO		2026-02-23
Reviewer (DPO)			
Reviewer (Engineering Lead)			
Approver	CEO		

Revision #3

Created 2026-02-24 22:50:54 UTC by John

Updated 2026-05-31 20:03:59 UTC by John