

DRAWING NO. KDV-2.0 - ARCHITECTURAL BLUEPRINT

Architectural Blueprint & Security Manifesto

100% ELLER INGENTING. INGEN BAKDØR.

Bygget for team som ikke har råd til at ett glemt passord — eller ett rettslig press mot oss — blir deres sikkerhetsbrudd.

Prosjekt	Ko Do · Vault — Zero-Knowledge Encryption Vault
Versjon	2.0 (2026-07)
Klassifisering	Offentlig — Arkitektur-blueprint
Regel	D-001 — 100% eller ingenting

100%

DOKUMENT

Architectural Blueprint & Security Manifesto

FOUNDER

Michael Aagreen

INSTANS

*.kodovault.no

01 Det Kompromissløse Paradigmet

THE ZERO-COMPROMISE PARADIGM

Nesten alle sikkerhetsløsninger på markedet i dag er bygget på en løgn: De ofrer sikkerhet for "convenience". De implementerer bakdører, passord-hint og server-side gjenoppretting fordi de er redde for å miste kunden hvis kunden glemmer passordet sitt. De opererer på en **95% sikkerhetsmodell**.

Ko|Do · Vault opererer utelukkende etter **Regel D-001: 100% eller ingenting**.

FOUNDER'S NOTE — REGEL D-001

"Spørsmålet er om det skal være 100% eller 95% — og svaret er 100%, ellers synker vi en eller annen dag, du vet bare ikke når."

— Michael Aagreen, Founder

Hvis en funksjon krever at vi må stole på "hjelpemekanismer" framfor ren matematikk, blir den ikke bygget. Glemmer en bruker master-passordet sitt, er dataene borte for alltid. Det er ingen "Glemt passord"-knapp. Det er ingen support-ingeniør som kan dekryptere hvelvet. Dette er ekte Zero-Knowledge.

For deg som kunde betyr det tre konkrete ting: **ingen insider-risiko** — ingen ansatt hos oss kan noensinne se dataene deres. **Ingen eksponering ved rettslig press** — vi kan ikke utlevere det vi selv ikke kan lese. Og **ingen enkelt svakhet** en angriper kan utnytte, fordi det ikke finnes en bakvei å angripe.

02 De Permanente Utelukkesene

THE ANTI-FEATURES

For å oppnå 100% teknisk ugjennomtrengelighet, har vi strukturelt og permanent eliminert følgende industristandarder:

- ✗ **Ingen klient-side expiry-sjekk i blob:** Ingen JavaScript-sjekker som kan forbigås i DevTools på 30 sekunder. Utløp og tilgang styres deterministisk.
- ✗ **Ingen soft-delete (papirkurv):** Når en fil, et passord eller et pass slettes, kjøres en umiddelbar, irreversibel destruksjon i databasen.
- ✗ **Ingen passive "Husk meg i 30 dager":** Ingen statiske tokens lagret i nettleseren som gir permanent tilgang.
- ✗ **Ingen passord-hint eller recovery-spørsmål:** Ingen sosiale sårbarheter (social engineering) tillates.
- ✗ **Ingen subdomene-basert "tillit":** URL-en gemini.kodovault.no betyr ingenting uten den kryptografiske master-nøkkelen. Kun master-passordet eier tilgangen.
- ✗ **Ingen backup uten passord:** Enhver eksport av data er kryptert med master-passordet. Det finnes ingen ukryptert backup-mekanisme, uavhengig av kontekst.

Konkurrentene kaller dette "brukervennlighet". Vi kaller det et sikkerhetshull.

FIG. 01 – ELIMINASJONSPRINSIPPET

INDUSTRIEN VS. KO|DO · VAULT

95% – INDUSTRIEN

- ✗ Passord-hint og recovery
- ✗ Server-side gjenoppretting
- ✗ Soft-delete med papirkurv
- ✗ Klient-side expiry (DevTools)
- ✗ Ukryptert backup

"CONVENIENCE"

100% – KO|DO · VAULT

- ✓ Kun master-passord (PBKDF2 600k)
- ✓ Zero-Knowledge – vi kan ikke lese
- ✓ Irreversibel destruksjon
- ✓ Deterministisk tilgangskontroll
- ✓ Kryptert backup, alltid

MATEMATIKK

DET FINNES INGEN MELLOMTING

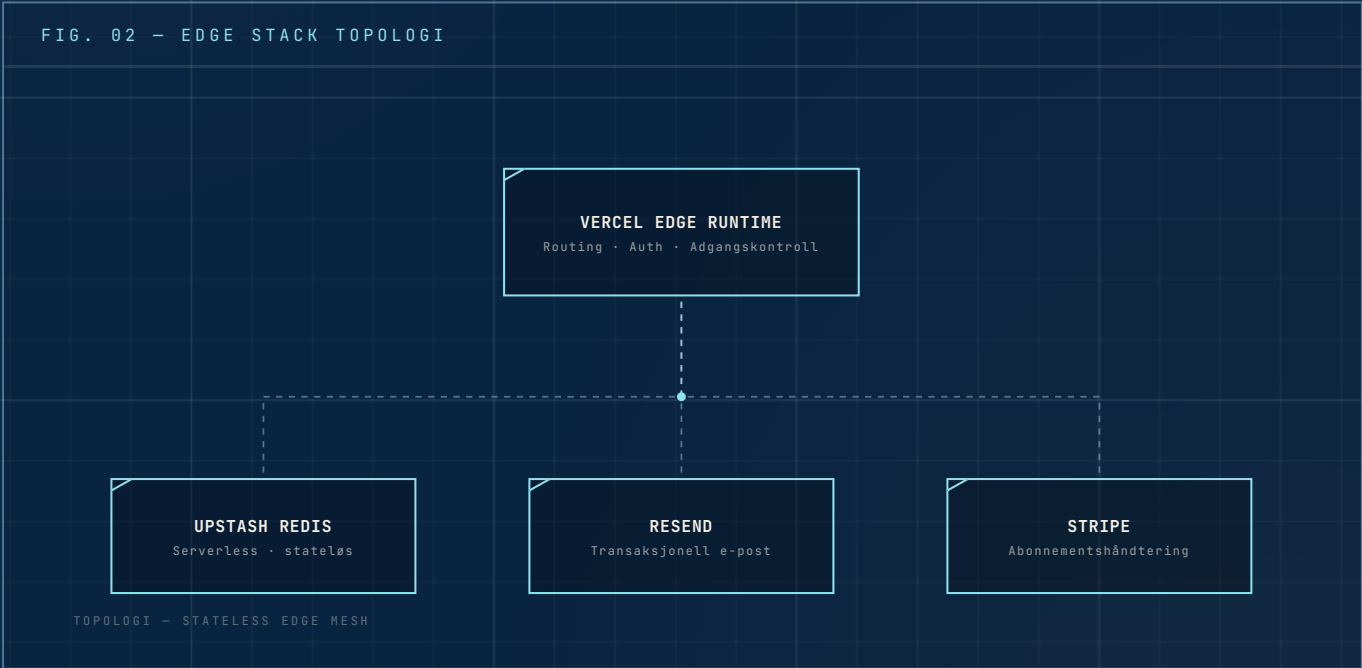
03 Stacken: Hyper-SaaS på Edge-nivå

THE EDGE STACK

Ko|Do · Vault er ikke bygget på trege, tradisjonelle databaseservere. Arkitekturen er en ultra-moderne, stateløs infrastruktur rigget for ekstrem hastighet og total isolasjon:

- **Vercel Edge Runtime:** All routing, autentisering og adgangskontroll skjer på "the edge" – millisekunder unna brukeren, før noen frontend-sider i det hele tatt rendres.
- **Upstash Redis (Serverless Database):** Brukes som et stateløst, lynraskt lager for de krypterte blob-ene. Siden tilkoblingen er stateløs, unngår vi åpne TCP-porter som hackere kan skanne eller angripe.
- **Resend & Stripe Integration:** Fullstendig integrert via sikre Edge-middleware API-er for transaksjonell kommunikasjon og multi-tenant abonnementshåndtering.

Tre-blob-arkitektur: Data separeres i tre uavhengige krypterte lag, hver med egen salt — passord (~50 KB, lastes alltid), kort (~3 MB, lastes ved behov), og ID-er (~5 MB, lastes ved behov). Blobs som ikke er åpnet, hentes aldri fra server. Kompromittering av én blob gir null innsyn i de andre.

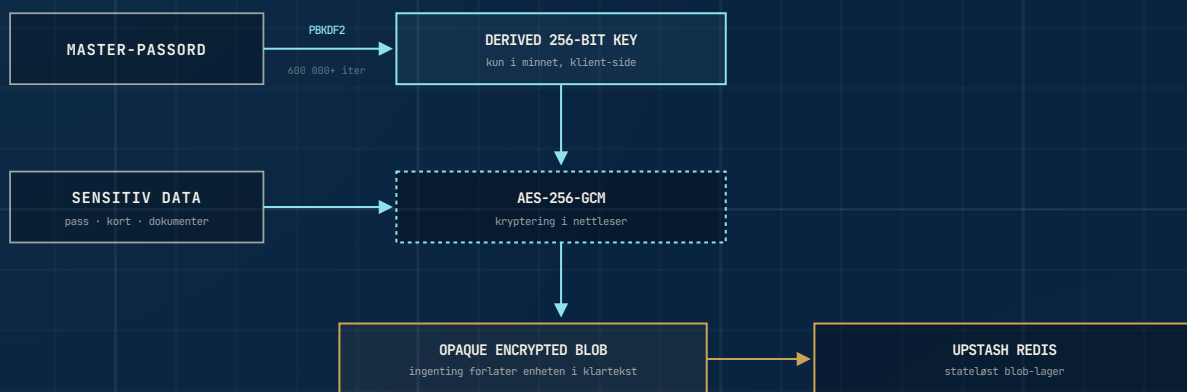


04 Den Kryptografiske Flyten

THE CRYPTOGRAPHIC FLOW

Når en bruker lagrer sensitive data (pass, kredittkort, sensitive dokumenter), forlater ingenting enheten i klartekst:

FIG. 03 – KRYPTOGRAFISK SKJEMA



SKJEMA – CLIENT-SIDE ZERO-KNOWLEDGE ENCRYPTION

Ko|Do · Vault inkluderer en innebygd **Password Lab** — en generator som bygger passord i flere formater: ord+ord-kombinasjoner, 12+ tegn med store og små bokstaver, eller inkludert spesialtegn. For hvert forslag vises estimert brute-force-tid i sanntid. Tallene er reelle: PBKDF2 med 600 000 iterasjoner gjør at hvert passord-forsøk koster 600 000 SHA-256-operasjoner. Med 1 000 toppmoderne GPU-er som jobber parallelt tar et 10-tegns alfanumerisk passord ~800 år å knekke. Et 12-tegns passord: over 3 millioner år. Selv om noen fikk tak i den krypterte bloben, er den matematisk verdiløs uten master-passordet.

Ingen app. Ingen installasjon. Tilgjengelig overalt. Ko|Do · Vault kjører 100% i nettleseren — Chrome, Safari, Firefox, Brave — på hvilken som helst enhet med internett. All kryptering og dekryptering skjer lokalt via Web Crypto API. Det finnes ingen native app som må installeres, oppdateres eller godkjennes av IT-avdelingen. Mister du lommebok, ID og laptop på reise? Med en lånt telefon, URL-en og master-passordet har du tilgang til alt — pass, kredittkort, ID-er — i løpet av sekunder. Alt ligger i skyen, kryptert, og venter på deg.

05 Multi-Tenant Rollebasert Sikkerhet

RBAC IN EDGE MIDDLEWARE

Systemet skiller knallhardt mellom tre unike administrasjonsnivåer direkte i Edge-middleware:

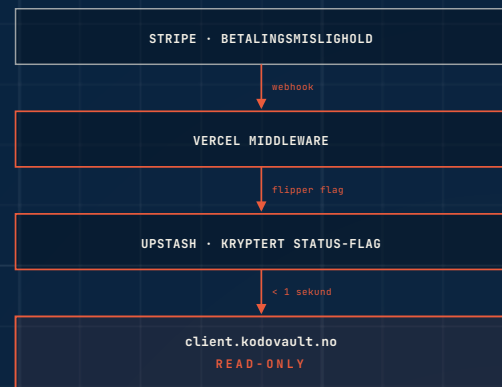
- 1 User:** Kan kun dekryptere og lese egne tildelte elementer.
- 2 Business Admin:** Administrerer lisenser, tilganger og delte bedriftsmapper.
- 3 Owner Admin:** Eier hele bedriftsinstansen (*.kodovault.no), styrer overordnet policy og håndterer Stripe-fakturering.

FIG. 04 – RBAC-HIERARKI



RBAC I EDGE-MIDDLEWARE – TRE NIVÅER

FIG. 05 – STRIPE DYNAMIC FREEZE



EDGE-NIVÅ FRYSING – INGEN SKRIVING MULIG

Stripe Dynamic Freeze: Hvis en bedriftskonto går i betalingsmislighold, skyter Stripe ut en webhook. Vercel Middleware plukker dette opp umiddelbart og flipper en kryptert status-flag i Upstash. På under ett sekund fryses hele instansen (**client.kodovault.no**) til en "Read-Only" tilstand på kanten (edge). Ingen data kan endres, manipuleres eller skrives før balansen er oppgjort.



D-001 Anvendt: Fire Operative Prinsipper

WHERE THE NORTH STAR MEETS REALITY

Filosofien i Seksjon 01 er ikke abstrakt — den styrer konkrete tekniske valg som mange leverandører unngår å snakke om. Her er fire eksempler.

- ▶ **Kamera som aldri rører Camera Roll:** Når en bruker fotograferer kredittkort eller pass i Ko|Do · Vault, brukes et custom kamera direkte i nettleseren. Bildet eksisterer **utelukkende i RAM**, krypteres der, og lagres i blob. Det rører aldri Camera Roll, aldri iCloud Photos, aldri Apples servere. Ingen konkurrent kommuniserer dette — fordi de fleste bruker standard fil-opplasting som lekker bildet til skylagring før det krypteres.
- ▶ **Clipboard-ærlighet (ingen falsk trygghet):** Web-plattformen kan **ikke** garantere 100% clipboard-tømming — Universal Clipboard synker til andre enheter, clipboard managers lagrer historikk, og en lukket fane stopper timeren. Vi er ærlige om dette. Løsningen: auto-tømming etter 120 sek + manuell "slett clipboard"-knapp + valgfri "tett skip"-modus der kopier-knappene fjernes helt. I tett skip-modus rører passordet aldri clipboard — brukeren leser det på skjerm og taster manuelt.
- ▶ **Biometrisk uten kompromiss:** Touch ID / Face ID tilbys kun på enheter der WebAuthn PRF faktisk fungerer kryptografisk (Safari 18+, Chrome 132+). På eldre enheter **skjules knappen helt** — i stedet for å tilby en svakere fallback. Heller ingen feature enn en 95%-feature.
- ▶ **Minimal klartekst-metadata:** Ved sikker overlevering (.kodoenc-filer) inneholder klartekst-headeren **kun** det mottakerens nettleser teknisk må ha for å derive nøkkel og dekryptere: KDF-parametre (salt, iterasjoner, algoritme) og cipher-parametre (IV, tagBits). Alt annet — tidsstempel, appversjon, filantall — er kryptert inne i pakken. Ingen fingerprint-data lekkes.

Hver av disse beslutningene kostet oss noe: ekstra utviklingstid, en funksjon som er litt mindre "magisk" for brukeren, eller en knapp som ikke vises på eldre enheter. Vi tok den kostnaden hver gang — fordi alternativet er at brukeren **tror** de er trygge uten å være det.

07 Sikker Overlevering — Filer og Mapper

ENCRYPTED HANDOVER

Brukeren velger filer eller hele mappestrukturer, setter et passord, og Ko|Do · Vault pakker alt i en **.kodoenc**-fil. Mottakeren åpner filen i nettleseren, taster passordet, og laster ned innholdet — uten konto, uten app, uten at filene noensinne berører en tredjeparts server i klartekst.

Dette erstatter e-postvedlegg, WeTransfer-lenker og delte Dropbox-mapper for alt som er sensitivt: kontrakter, ID-dokumenter, økonomiske rapporter, helseinformasjon. Mottakeren trenger kun en nettleser og passordet — som deles via en separat kanal.

- ▶ **Filer og mapper:** Ikke bare enkeltfiler — hele mappestrukturer pakkes og krypteres med bevart hierarki. Mottakeren får tilbake nøyaktig samme struktur ved dekryptering.
- ▶ **Klient-side kryptering:** Filene krypteres i avsenderens nettleser før de forlater enheten. Serveren ser aldri innholdet — kun den krypterte .kodoenc-pakken.
- ▶ **Ingen konto for mottaker:** Mottakeren trenger ikke en Ko|Do · Vault-konto, ingen registrering, ingen app-installasjon. Åpne lenken, tast passord, last ned.
- ▶ **Minimal metadata:** Klartekst-headeren inneholder kun det teknisk nødvendige for dekryptering (salt, IV, iterasjoner). Filnavn, antall, størrelse og tidsstempel er kryptert inne i pakken.

For B2B-kunder: En advokat sender saksdokumenter til klienten. En regnskapsfører sender årsoppgjøret. En HR-avdeling sender ansettelseskontrakter. I alle tilfeller: ett passord, én .kodoenc-fil, null eksponering.

08 Hva Om Vi Forsvinner? ZERO VENDOR LOCK-IN

De fleste sikkerhetsleverandører unngår dette spørsmålet. Vi svarer på det direkte.

Når en bruker sender en kryptert pakke (.kodoenc) til en mottaker, er mottakerens dekrypteringsflyt **100% klient-side JavaScript**. Ingen backend-kall, ingen analytics, ingen tredjepartsskript. Hvis Ko|Do legges ned i morgen, fungerer pakken fortsatt — fordi den aldri trengte oss. Dette er et **arkitekturelt prinsipp**:

- ▶ **Null server-kall fra mottaker-ruten** — kun statisk JavaScript som kjører i mottakerens nettleser.
- ▶ **Null tracking eller telemetri** — fungerer i Brave med strict tracking-protection, Firefox, Safari, alle browsere.
- ▶ **Dokumentert filformat** — .kodoenc kan implementeres på nytt med standard Web Crypto API (PBKDF2 + AES-GCM) av enhver utvikler.
- ▶ **Ingen WebAuthn, ingen Upstash, ingen Stripe** på mottaker-siden — mottakeren trenger ikke en konto, ikke en relasjon med oss, ikke engang internett etter første sidelasting.

For deg som B2B-kunde betyr dette: Dine ansatte kan sende krypterte filer til klienter, motparter og samarbeidspartnere som aldri trenger å vite hva Ko|Do · Vault er. Mottakeren trenger kun passordet og en nettleser. **Praktisk — hvis Ko|Do ikke lenger eksisterer:**

- 1 Har mottakeren åpnet /unpack-siden tidligere, ligger den i nettleserens cache (PWA). Dekryptering fungerer offline — ingen server nødvendig.
- 2 Filformatet (.kodoenc) er fullt dokumentert. Enhver utvikler kan reimplementere dekrypteringen med standard Web Crypto API: PBKDF2-SHA256 (600k iter) → AES-256-GCM. Headeren inneholder alle nødvendige parametre.
- 3 Vault-data (passord, kort, ID-er) er krypterte blobs i Upstash Redis. Med master-passordet og blobbens rå-data kan innholdet dekrypteres med samme kryptoprimitiver — uavhengig av Ko|Do.

DETTE ER IKKE EN FEATURE-LISTE. DET ER EN GARANTI.

Klar for en vault som aldri kompromitterer? Opprett din egen på kodovault.no — eller ta kontakt for en teknisk gjennomgang av arkitekturen med teamet ditt.