Sikkerhet

Sist oppdatert 11. mai 2026. Versjon 1.3.

Teknisk oversikt over hvordan DigiReq beskytter brukerne og dataene deres. Skrevet for IT-revisjon hos kommunale kunder. For forretningsmessig kontekst, se personvernerklæring og databehandleravtale.

1. Arkitektur

2. Hosting og lokasjon

- **Server og database:** Hetzner Online GmbH, datasenter Helsinki, Finland (EU/EØS).
- **Backup:** Hetzner snapshots — kryptert, samme region, daglig retensjon (7 stk).
- **Edge / DNS:** Cloudflare (kun proxy, ser ikke applikasjonsdata i klartekst).
- **Landingsside:** Netlify (statisk, ingen brukerdata).
- Komplett liste over underleverandører: /underleverandorer.

3. Transport og kryptering

- TLS 1.2 og 1.3 med moderne chiffer-suiter — ingen SSLv3, TLS 1.0 eller 1.1.
- HSTS aktivert (`max-age=31536000; includeSubDomains`) — tvinger HTTPS i nettleser.
- Sertifikater fra Let's Encrypt med automatisk fornyelse via certbot.
- Database-tilkoblinger fra applikasjonen er over lokalt loopback (127.0.0.1).

4. Autentisering

DigiReq støtter to autentiseringsmetoder, valgt per rolle og per organisasjon:

- **Microsoft Entra ID (OIDC)** — for admin og godkjenner-roller. Kunden kan slå av SMS-OTP helt for disse rollene («Entra ID-only»-modus), eller la begge metodene stå som fallback. Ansatte i felt beholder SMS uansett.
- **SMS engangskode (OTP)** — primær for ansatte i felt; fallback for admin/godkjenner når Entra ID ikke er konfigurert eller kunden velger det.

4.1 Microsoft Entra ID OIDC

- **Standard OpenID Connect** Authorization Code Flow med PKCE (S256 challenge fra 64-byte URL-safe random verifier). Multi-tenant app-registrering — hver kunde gir admin-consent fra egen tenant.
- **Tenant-isolasjon** håndheves per pålogging: ID-tokenets `iss`- og `tid`-claims må matche kundens registrerte tenant-ID. Et token signert av en annen tenant blir avvist selv om signaturen ellers er gyldig.
- **State-cookie:** Signert med `SECRET_KEY` + salt (itsdangerous URLSafeTimedSerializer), 10 min TTL, attributter `HttpOnly`, `Secure`, `SameSite=Lax`,`Path=/auth`. Beskytter mot CSRF og replay-angrep.
- **JWKS host-pinning:** Discovery-doc og JWKS hentes kun fra `https://login.microsoftonline.com`; også `authorization_endpoint` og `token_endpoint` valideres mot samme host før bruk. Hindrer at en poisoned discovery-respons kan omdirigere oss til en angriper-server.
- **ID-token-validering:** Signatur (RS256) mot tenant- spesifikk JWKS (cachet 1 time), `exp`/`iat`/`nbf` med 60 sek klokke-skew-toleranse, `aud` mot vår client ID, `nonce` mot signed state, og at `oid` finnes.

- **Minimum-rettigheter:** Kun tre standard OIDC-scopes — `openid`, `profile`, `email`. Vi leser ikke kalender, filer, mailbox eller Teams. Microsoft-konto-IDen (`oid`) lagres som referanse for brukerkobling — ingen passord eller token er persistert hos oss utover sesjonen.
- **Invite-only linking:** Bruker må være forhåndsinvitert av en admin (e-postadresse matchet i DigiReq-databasen) før første OIDC-login. Random Microsoft-kontoer kan ikke logge inn — ingen self-service registrering.
- **Fragment-redirect** for tokens: backend sender JWT tilbake til frontend som `#access=…&refresh=…` i URL- fragmentet. Fragmenter sendes ikke til server, så tokens lekker ikke til access-logger. Frontend strippes fragmentet umiddelbart via `history.replaceState` for å forhindre replay via browser-historikk, og validerer tokens med en eksplisitt `Authorization`-header mot `/auth/me` før de persisteres i `localStorage`.
- **Tilbakekall:** Kunde-IT kan trekke samtykket fra Microsoft Entra → Enterprise applications → DigiReq → Delete når som helst. Effekt umiddelbar; SMS-OTP-brukere er ikke berørt.
- **Kunde-IT-guide:** /admin/consent genererer en signert admin-consent-URL kunde-IT bruker for å aktivere DigiReq i sin tenant. Tre klikk fra mottatt e-post til ferdig oppsett.

4.2 SMS engangskode (OTP)

- **Leverandør:** 46elks (Sverige), EU/EØS — ikke overføring.
- **OTP-håndtering:** Hash-es med bcrypt (kostfaktor 10). Lagres aldri i klartekst. TTL 5 minutter. Maks 5 feil-forsøk per OTP.
- **Per-org policy:** Hvis kunden har slått på `require_oidc_for_admin`, avvises SMS-OTP for admin- og godkjenner-rollene med klar feilmelding som peker dem mot Microsoft-knappen. Sjekken skjer FØR OTP-koden konsumeres — koden brennes ikke på en policy-feil.

4.3 MFA-policy for admin- og godkjenner-roller

DigiReq anbefaler sterkt at **admin- og godkjenner-tilgang krever multi-faktor autentisering (MFA)**. MFA håndheves i kundens egen Microsoft Entra-tenant via Conditional Access, ikke i DigiReq. Det gir kundens IT full kontroll over policy, MFA- metoder (Authenticator, FIDO2, sertifikat) og revokering.

Anbefalt Conditional Access-policy for DigiReq-app-en:

- **Krav om MFA** ved hver pålogging eller på risiko-basert nivå (Identity Protection).

- **Sesjons-kontroll:** tidsbegrenset pålogging (f.eks. 8-12 timer) og re-autentisering ved nye enheter.
- **Valgfritt:** krav om kompatible/registrerte enheter (Intune-managed) for ekstra device-binding.
- **Valgfritt:** lokasjons-restriksjon hvis kommunal IT har geografiske krav.
- **Anbefalt:** blokker legacy-autentisering (ikke aktuelt for DigiReq, men hygiene-tiltak).

For å håndheve at admin/godkjenner KUN kan logge inn via Entra (og dermed MFA-policyen), slå på `require_oidc_for_admin` i admin-dashbordet under Firma-innstillinger. SMS-OTP avvises da for privilegerte roller med en feilmelding som peker dem til Microsoft-pålogging. Employee-rollen (felt-ansatte) kan fortsette med SMS-OTP siden rekvisisjons-opprettelse alltid må gjennom godkjenner-flowen før EHF-ordre genereres.

4.4 Sesjon

- **JWT:** Access-token (60 min, HS256) + refresh-token (60 dager). Tokens er ikke regokneliggjørbare server-side; rolle er innbakt i access-claim slik at decorators kan håndheve uten ny DB-spørring.
- **Lagring i mobilapp:** iOS Keychain / Android Keystore — aldri i klartekst.
- **Lagring i admin-dashboard:** `localStorage` — kun for HTTPS-origin `digireq.no`.
- **Deaktivering av bruker** (`is_active=false`) blokkerer både access-token-verifisering og refresh; effekten er umiddelbar ved neste forespørsel.
- **Biometri (valgfritt mobil-app):** Face ID / fingeravtrykk validert lokalt på enheten — biometriske data forlater aldri telefonen. Biometric-login respekterer samme `require_oidc_for_admin`-policy som SMS-OTP.

5. Tilgangskontroll

Rollebasert tilgangskontroll med fire nivåer, håndhevet både i backend (decorator-nivå) og frontend (UI-nivå):

- **employee:** oppretter rekvisisjoner; ser kun sine egne.
- **approver:** godkjenner/avviser i sin avdeling; ser sin avdelings rekvisisjoner.
- **admin:** per-firma admin; brukere, avdelinger, terskler, audit-logg.
- **super_admin:** plattform-eier; oppretter firmaer + tildeler første admin. Har **ikke** automatisk tilgang til kunders rekvisisjons-data på tvers av firmaer.

Tenant-isolasjon på `company_id` — alle data-spørringer er scoped til brukerens firma, håndhevet i backend.

6. Rate-limit og misbruks-beskyttelse

- **Autentiserings-endepunkter** (OTP, login): 10 forsøk/min per IP.
- **API-endepunkter:** 300 req/min per autentisert bruker (JWT-basert) — kommunenett bak NAT deler ikke samme bucket.
- **OTP-spesifikt:** Maks N OTP-koder per telefon per time (beskytter SMS-budsjett).
- **Cloudflare DDoS** foran applikasjonen.
- **HTTP 429** med korrekt status til klienter — håndteres grasiøst i app/dashboard.

7. Drift og monitorering

- **SSH:** Kun ed25519 nøkkel-autentisering. Passord-login deaktivert. Tilgang begrenset til Tailscale-nettverk via UFW (port 22 stengt mot internett).
- **Brannmur:** UFW aktiv — kun port 80 og 443 åpne mot internett.
- **Fail2ban** aktiv mot brute-force på SSH (om noe slipper inn via Tailscale).
- **Sikkerhetsoppdateringer:** unattended-upgrades aktivert — kritiske patches installeres automatisk.
- **Sårbarhetshåndtering:** CVE-overvåkning og avhengighets-oppdateringer i CI-flyt.
- **Tilgangs-revisjon:** Manuell gjennomgang av SSH-nøkler hver 6. mnd; rotasjon ved personalendringer.

8. EHF-integrasjon (Peppol BIS Order 3.0)

Når en rekvisisjon godkjennes, kan DigiReq sende dokumentet som en standardisert **EHF Order (Peppol BIS 3.0)** til kundens innkjøps-/ERP-system (typisk Visma e-handel eller tilsvarende), som internt sørger for at fakturamottaket matcher leverandørfakturaen mot ordren. Dette er åpen standard, ikke et proprietært format — samme struktur som hver eneste norske leverandør bruker for EHF-fakturaer i dag.

- **Format-validering:** Hver utgående fil valideres mot OpenPeppol BIS Order 3.0 schematron (XSD + business rules) før leveranse. Avvist input feiler tidlig — kunden mottar aldri en ugyldig fil.

- **Norske org-nr:** Mod-11-validering på buyer/seller org-nr (PEPPOL-COMMON-R041) hindrer fil-leveranse med ugyldig norsk identifikator.
- **Tre leveranse-kanaler** — kunden velger (Peppol er anbefalt default):
  - **Peppol AP (Tickstar Galaxy):** Vi sender via DigiReqs Peppol Access Point. AS4-transport mellom AP-er er signert og kryptert i tråd med Peppol-spesifikasjonen. Avsender-identitet er kundens org-nr (`0192:<org>`), mottakerens AP slås opp via SMP. Tickstar driver AP-en på vår vegne — vi har databehandleravtale med dem og de er ført opp som underleverandør på /underleverandorer.
  - **SFTP:** Vi laster opp fil til kundens SFTP-server. Autentisering med ed25519-nøkkel-par per kunde (vi genererer, kunden installerer offentlig nøkkel). Atomic upload via `.tmp`-fil + `posix_rename` hindrer halv-skrevne filer.
  - **SFTP host key pinning (TOFU):** Vi pinner serverens host key på første vellykkede tilkobling og verifiserer mot pinnet fingerprint før vi presenterer vår private signatur ved hver påfølgende leveranse. Avvik avbryter leveransen — beskytter mot DNS-poisoning og MITM-angrep mot SFTP-hostnamn.
  - **HTTPS-webhook:** Kun `https://`-URL aksepteres — `http://` avvises både ved konfigurasjon og ved leveranse (defence-in-depth). Vi POSTer XML-kropp med `X-DigiReq-Signature: sha256=…`-header. Kunden verifiserer i konstant tid med delt HMAC-secret.
  - **Webhook replay-beskyttelse:** HMAC-en signeres over `timestamp + "\n" + body`, ikke bare body. En forespørsel kan ikke replayes med en fersk timestamp-header. Kunden bør avvise meldinger eldre enn 5 minutter.
- **Inn-validering:** SFTP-brukernavn og `target_path` valideres mot whitelist (POSIX-sikre tegn, `..` avvist). Webhook-URL må være HTTPS. Norske org-numre må passere mod-11-check (`PEPPOL-COMMON-R041`).
- **Self-service oppsett:** Kunde-admin konfigurerer kanal og destinasjon på `/admin/integration`. Vi genererer credentials automatisk; kunden trenger ikke håndtere kryptografi selv.
- **Kryptering av credentials:** SSH-privatnøkler og webhook-secrets lagres fernet-kryptert (AES-128-CBC + HMAC-SHA256) med en HKDF-SHA256-derivert nøkkel fra `SECRET_KEY` (i miljøvariabel, ikke i database). En ren database-dump avslører ikke noen credentials.
- **Aldri eksponert:** Etter opprettelse returnerer ingen API-endpoint privat-nøkkel eller webhook-secret i klartekst — kun ved første-opprettelse eller eksplisitt rotering via

`/admin/integration/rotate`. Rotering tar row-lock så samtidige rotasjoner ikke overskriver hverandre.

- **Audit-logget:** Hver leveranse (vellykket eller feilet) registreres i audit-loggen med kanal, destinasjon, tidsstempel og status. Synlig for kunden.
- **Test-flyt:** Synthetic test-leveranse via `/admin/integration/test` verifiserer setup uten å sende ekte rekvisisjons-data.

Implementasjons-detaljer (lxml + paramiko + cryptography) er gjengs blant offentlige norske aktører og kan revideres. Kontakt sikkerhet@digireq.no for tekniske spørsmål.

9. Audit-log og sporbarhet

- Append-only `audit_log`-tabell logger hver write-handling: bruker-invitasjon, rolle-endring, godkjenning, avslag, plattform-handlinger.
- Hver rad inneholder: tidspunkt, hvem (bruker), handling, detaljer (CRLF-strippet for å forhindre log-injection), IP, tenant.
- Tilgjengelig for kunde-admin via `/admin/audit` — søk, filter, CSV-eksport.
- Oppbevaring: 12 måneder, deretter automatisk sletting via cron-jobb.
- Plattform-handlinger fra super_admin flagges automatisk som "krever oppmerksomhet" i kundens audit-visning — full transparens.

10. Sikkerhetsbrudd-prosedyre

- Kunden varsles innen 24 timer ved kjennskap til brudd, jf. databehandleravtale §10.
- Varselet inneholder informasjonen kunden trenger for å oppfylle sin meldeplikt til Datatilsynet (innen 72 timer per GDPR art. 33).
- Post-mortem-rapport innen 7 dager etter løsning — root cause, tiltak, forebygging.

11. Sikker utvikling

- Hemmeligheter (API-nøkler, JWT-secret, DB-passord) lagret i miljøvariabler — aldri i kildekode eller versjonskontroll.
- Avhengigheter overvåkes kontinuerlig via GitHub Dependabot. CVE-varsler genereres ved kjente sårbarheter i tredjeparts-biblioteker, og sikkerhets-patcher rulles ut via

automatiske pull requests gruppert per økosystem. Sårbare versjoner oppdateres innen 7 dager (kritiske: 24 timer).

- Kildekode i privat Git-repo med to-faktor-autentisering på alle utviklere.
- Deploy via signert push fra navngitt utvikler; ingen direkte produksjons-tilgang for andre.
- **AI-verktøy i utvikling:** Vi bruker Anthropic Claude som kode-assistent under utvikling (sammenlignbart med GitHub Copilot eller tilsvarende). **Ingen kundedata, personopplysninger eller produksjons-secrets sendes til AI-tjenester** — kun kode-snippets og generelle utviklings-spørsmål. Anthropic er derfor ikke databehandler for DigiReq-tjenesten i GDPR-forstand (jf. Art. 28), og står ikke påunderleverandør-listen. AI-bruken er en utvikler-side-praksis, ikke en produksjons-komponent.

12. Kontakt

Sikkerhets-relaterte henvendelser, ansvarlig avsløring av sårbarheter, eller spørsmål til IT-revisjon: sikkerhet@digireq.no.

Dokument-versjon 1.5 · Sist oppdatert 29. mai 2026 · sikkerhet@digireq.no

Endringslogg

- **1.5 (29. mai 2026):** Seksjon 11 (Sikker utvikling) presiserer at AI-verktøy (Anthropic Claude) brukes som kode-assistent uten at kundedata eller persondata sendes — Anthropic er derfor ikke databehandler i GDPR-forstand.
- **1.4 (29. mai 2026):** Ny seksjon 4.3 dokumenterer MFA- policy for admin- og godkjenner-roller: anbefalt baseline er Microsoft Entra ID med Conditional Access (MFA, sesjons-kontroll, valgfri device compliance), håndhevet per firma via `require_oidc_for_admin`. Eksisterende 4.3 Sesjon flyttet til 4.4. Seksjon 11 (Sikker utvikling) presiserer at avhengigheter overvåkes via GitHub Dependabot med automatiske, grupperte sikkerhets- PR-er per økosystem.
- **1.3 (11. mai 2026):** Utvidet seksjon 4 (Autentisering) med Microsoft Entra ID OIDC for admin/godkjenner-roller — multi-tenant app, PKCE S256, JWKS host-pinning, tenant-isolasjon, signed state-cookie, invite-only linking, fragment-redirect for tokens. Lagt til per-org policy `require_oidc_for_admin`. Oppdaterte JWT-TTL-tall (60 min / 60 dager) til faktiske produksjonsverdier.

- **1.2 (8. mai 2026):** Lagt til detaljer i seksjon 8 etter intern sikkerhetsgjennomgang av EHF-integrasjonen: SFTP host key pinning (TOFU mot MITM), HTTPS-only-håndhevelse for webhook, replay-beskyttelse via timestamp i HMAC-signaturen, inn-validering av brukernavn/path/URL, row-lock på rotering.
- **1.1 (8. mai 2026):** Lagt til seksjon 8 om EHF/Peppol-leveranse — SFTP og webhook-kanaler, fernet-kryptering av credentials, mod-11 org-nr-validering, audit-logging av leveranser. Renumrert seksjon 9-12.
- **1.0 (6. mai 2026):** Første publiserte versjon.

OM LEVERANDØREN

Tjenesten DigiReq leveres av **Påvakt AS** (org.nr. **937 620 187**), heretter omtalt som «Leverandør». DigiReq er registrert som virksomhet under Påvakt AS (**Digireq**, org.nr. **937 700 539**). Avtaler signeres med Påvakt AS som juridisk enhet; EHF-fakturaer fra DigiReq utstedes på Digireqs virksomhets-org-nr.

Kontakt: info@digireq.no · Sikkerhet: sikkerhet@digireq.no · Personvern: personvern@digireq.no