API-dokumentasjon

Oversikt over DigiReqs REST API. Full endepunkts-spesifikasjon leveres til faktiske integrasjons-kunder under taushetsavtale.

> **Status:** API-et drifter våre egne klienter (mobil-app + admin-dashbordet). Full OpenAPI-spesifikasjon leveres på forespørsel til kunder som skal bygge egen integrasjon. Denne siden gir et høyere-nivå overview slik at kommune-IT kan vurdere arkitekturen og sikkerhets- modellene før integrasjons-prosjekt startes.

1. Grunnleggende

- **Base-URL:** `https://api.digireq.no`
- **Format:** JSON (request og response)
- **Transport:** HTTPS (TLS 1.2+) påkrevd; HTTP omdirigerer til HTTPS
- **Tegnsett:** UTF-8
- **Tidsstempler:** ISO-8601 i UTC
- **Telefon-numre:** E.164-format

2. Autentiserings-modeller

Tre måter å autentisere mot API-et, valgt etter use-case:

2.1 JWT (mobil + admin-dashboard)

- Standard for våre egne klienter
- Token hentes etter SMS-OTP eller Microsoft Entra ID-pålogging
- Sendes som `Authorization: Bearer <token>`-header
- Access-token TTL 60 minutter, refresh-token TTL 60 dager
- Tokens revokeres umiddelbart ved `is_active=false`

2.2 Webhook HMAC (kunde-integrasjon)

- For at kunde-systemer skal verifisere ekthet på innkommende webhooks fra DigiReq
- HMAC-SHA256 over `timestamp + body` i `X-DigiReq-Signature`-header
- Replay-beskyttelse via timestamp; klienten bør avvise meldinger eldre enn 5 minutter
- Delt secret per kunde, distribueres ved oppsett

2.3 OIDC / Microsoft Entra ID

- For admin-pålogging via SSO
- PKCE S256 + signed state cookie for CSRF-beskyttelse
- JWKS host-pinning til `login.microsoftonline.com`
- Tenant-isolasjon validert per pålogging
- Full oppsetts-guide: /sso-entra-id

3. Funksjons-områder

API-et er strukturert i funksjons-grupper. Konkrete endepunkts-stier deles ikke offentlig — full spesifikasjon leveres til integrasjons-kunder under taushetsavtale.

- **Autentisering** — SMS-OTP, biometri, OIDC, token-refresh
- **Rekvisisjoner** — opprett, hent, godkjenn, avvis, bekreft faktisk beløp, markér brukt i butikk
- **Admin** — bruker-administrasjon, avdelinger, terskler, audit-logg, EHF-leveranse-konfigurasjon
- **EHF-integrasjon (utgående)** — konfigurere SFTP, HTTPS-webhook eller Peppol AP for ordre-leveranse
- **Self-service onboarding** — Brreg-oppslag, signup, setup-wizard, CSV-import av brukere
- **Billing-admin** — abonnement-status, trial-bekreftelse, reaktivering fra pause
- **Helse** — offentlig `/health`-endepunkt for ekstern monitorering

For utgående EHF-format og leveringsalternativer, se /ehf-integrasjon.

4. Rate-limit og DDoS-beskyttelse

- Cloudflare DDoS-beskyttelse foran applikasjonen
- Rate-limit på autentiserings-endepunkter (per IP + per telefonnummer)
- Generelt API-tak per JWT
- Ved overskridelse: `429 Too Many Requests` med `Retry-After`-header

5. Feil-håndtering

Standard HTTP-status-koder. Feil-respons følger formatet:

```
{
  "error": "<error_code>",
  "message": "<menneskelesbar beskrivelse>",
  "details": { ... }   // valgfritt, kontekst
}
```

Typiske feil-koder: `invalid_input`, `unauthorized`, `forbidden`, `not_found`, `conflict`, `oidc_required`, `rate_limited`, `internal_error`.

6. Idempotens

Skrive-operasjoner som kan re-prøves støtter `Idempotency-Key`-header (UUID). Respons cachet i 24 timer per nøkkel. Bruk samme nøkkel ved retry for å unngå duplikater.

7. Sikkerhet og audit

- Alle privilegerte handlinger logges i append-only audit-log med actor + IP + tidsstempel
- Personopplysninger håndteres per DPA
- Tekniske sikkerhets-detaljer: se /sikkerhet

8. Versjonering og bakoverkompatibilitet

- **Bakoverkompatible endringer** (nye optional felt) skjer uten varsel
- **Ikke-bakoverkompatible endringer** introduseres med ny versjons-prefiks og minimum 6 måneders parallell-drift
- Kunder med aktiv integrasjon varsles minst 30 dager før breaking changes

9. Få tilgang til full spesifikasjon

For å bygge integrasjon mot DigiReq trenger du:

1. Aktivt kundeforhold til DigiReq (trial eller betalt)
2. Signert tilleggsavtale om integrasjons-tilgang (taushetsplikt på endepunkts-detaljer)
3. Generert API-credentials av Leverandør

Ta kontakt på info@digireq.no for å sette opp integrasjons-prosjekt. Vi leverer da OpenAPI 3.1-spesifikasjon, sandbox-tilgang og teknisk veiledning.

10. Kontakt

- **Integrasjons-spørsmål:** info@digireq.no
- **Sikkerhets-spørsmål:** sikkerhet@digireq.no
- **EHF/Peppol-detaljer:** /ehf-integrasjon

Dokument-versjon 0.2 · Sist oppdatert 29. mai 2026 (scrubbed til overview; full spesifikasjon under NDA) · info@digireq.no

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