ADR-007: BankID OIDC Auth

ADR-007: BankID as Sole Authentication Provider

Status: Accepted **Date:** 2026-02-21 **Deciders:** Alem (CEO), John (AI Director) **Category:** Security

---

Context

Drop is a financial application operating under PSD2 in Norway. PSD2 mandates Strong Customer Authentication (SCA) for payment initiation and account access. SCA requires two of three factors: knowledge (something you know), possession (something you have), and inherence (something you are).

Authentication options considered:

Option	SCA Compliant	KYC Built-in	Norwegian Coverage	Implementation
BankID	Yes (possession + knowledge/biometric)	Yes (national ID verified)	~4.5M users (90%+ adult pop.)	OIDC standard
Vipps Login	Partial (depends on config)	Partial (phone-verified)	~4.3M users	OIDC standard
Email + Password	No (single factor)	No	Universal	Simple
Email + OTP	Partial (possession)	No	Universal	Medium

BankID provides the strongest combination: SCA compliance (BankID app = possession, PIN = knowledge, biometric = inherence), built-in identity verification (national ID / fodselsnummer), and near-universal adoption in Norway. Using BankID as the sole auth provider eliminates the need for a separate KYC step -- identity is verified at login.

The original Drop codebase used email + password authentication, which is inadequate for PSD2 compliance and provides no identity verification.

Decision

Use BankID OIDC as the sole authentication provider for Drop. Remove email/password login.

Authentication architecture:

Platform	Flow	Token Storage	Token Lifetime
Web (Next.js BFF)	BankID OIDC redirect flow	httpOnly cookie (`drop_token`)	7 days
Mobile (Expo)	BankID OIDC with deep link callback	AsyncStorage (Bearer token)	7 days

User creation is automatic on first BankID login:

1. Parse `pid` (fodselsnummer, 11 digits) from BankID ID token
2. Hash `pid` with SHA-256 for storage (`national_id_hash` column)
3. Check for existing user by `national_id_hash`
4. If new: create user with `kyc_status = 'approved'`, `kyc_method = 'bankid'`
5. Verify age >= 18 from `pid` birthdate encoding

```
sequenceDiagram
    participant User
    participant Drop as Drop (BFF)
    participant BankID as BankID OIDC

    User->>Drop: GET /api/auth/bankid
    Drop->>Drop: Generate state + nonce
    Drop->>Drop: Set bankid_state cookie
    Drop->>User: Redirect URL to BankID

    User->>BankID: Authenticate (app/code device)
    Note over User,BankID: SCA: possession (device) +<br/>knowledge (PIN) or inherence
(biometric)
    BankID->>User: Redirect to callback with code

    User->>Drop: GET /api/auth/bankid/callback?code=&state=
    Drop->>Drop: Verify state vs cookie
    Drop->>BankID: Exchange code for tokens
    BankID->>Drop: ID token + access token
    Drop->>Drop: Verify ID token (JWKS)
```

```
    Drop->>Drop: Extract pid, verify age >= 18
    Drop->>Drop: Find or create user
    Drop->>Drop: Create session, set JWT cookie
    Drop->>User: 302 Redirect to /dashboard
```

Deprecated endpoints (return 410 Gone):

- `POST /auth/login` -- replaced by BankID OIDC
- `POST /auth/register` -- automatic via BankID
- `POST /auth/verify-otp` -- not needed

Consequences

Positive

- Full PSD2 SCA compliance out of the box
- Identity verification (KYC) built into authentication -- no separate KYC step for basic verification
- Near-universal adoption in Norway (~4.5M BankID users)
- Eliminates password-related attack vectors (credential stuffing, brute force, phishing)
- National ID hash enables user deduplication across auth providers (Vipps in Phase 2)
- Industry-standard OIDC protocol -- well-documented, well-supported

Negative

- Users without BankID cannot use Drop (excludes some demographics: very young, recent immigrants)
- Dependency on BankID infrastructure availability
- BankID integration requires BankID Norge agreement and certificate
- Development requires mock OIDC flow (`BANKID_MOCK=true`) since real BankID needs production credentials
- More complex auth flow compared to email/password

Risks

- **BankID outage:** If BankID is down, no one can log in. Mitigation: Vipps Login planned as Phase 2 fallback (`auth_provider` field supports multiple providers).
- **Demographic exclusion:** Users without BankID (e.g., new residents) cannot register. Mitigation: Vipps Login + Sumsub manual KYC as alternatives in Phase 2.

References

- Authentication System -- Full auth implementation documentation
- BankID OIDC Integration -- Integration specification
- ADR-004: JWT httpOnly Cookies -- Token storage decision
- ADR-003: PSD2 Pass-through -- SCA requirement origin
- Security Architecture -- Session management details
- BankID Norge OIDC documentation

Revision #5
Created 2026-02-21 05:58:59 UTC by John
Updated 2026-05-23 10:56:44 UTC by John