Authentication

Drop Authentication System

> Sources: `src/drop-app/src/app/api/auth/bankid/`, `src/drop-api/src/lib/bankid.ts`, `src/drop-api/src/routes/auth.ts`

Overview

Drop uses **BankID OIDC** as the sole authentication method. Email/password login has been removed to comply with PSD2/SCA requirements.

- **Auth method:** BankID OIDC (Norwegian eID)
- **JWT Algorithm:** HS256 (HMAC-SHA256), RS256 opt-in
- **Library:** `jose` (`SignJWT` / `jwtVerify`)
- **Token lifetime:** 24h (web cookie), 7d (mobile Bearer token)
- **Web cookie:** `drop_token` (httpOnly, secure, sameSite=strict)
- **Mobile:** Bearer token in Authorization header

Phase 2 (planned)

- Vipps Login — same OIDC pattern, user dedup by `national_id_hash`
- Idura aggregator optional (single integration point for BankID + Vipps)

Authentication Flow

BankID Login (Web)

```
Browser                    Next.js BFF                  BankID OIDC
  |                            |                            |
  |  GET /api/auth/bankid      |                            |
```

```
  |--------------------------->|                              |
  |                            |  1. Rate limit check         |
  |                            |  2. Generate state + nonce   |
  |                            |  3. Set bankid_state cookie  |
  |  { redirectUrl }           |                              |
  |<---------------------------|                              |
  |                            |                              |
  |  Browser redirects to BankID authorize URL                |
  |---------------------------------------------------------->|
  |                            |                              |
  |  User authenticates with BankID                           |
  |                            |                              |
  |  BankID redirects to /api/auth/bankid/callback?code=&state=
  |<----------------------------------------------------------|
  |                            |                              |
  |  GET /callback?code&state  |                              |
  |--------------------------->|                              |
  |                            |  4. Verify state vs cookie   |
  |                            |  5. Exchange code for tokens |
  |                            |----------------------------->|
  |                            |  { id_token, access_token }  |
  |                            |<-----------------------------|
  |                            |  6. Verify ID token (JWKS)   |
  |                            |  7. Parse pid, verify age    |
  |                            |  8. Find/create user         |
  |                            |  9. Create session + cookie  |
  |  302 /dashboard            |                              |
  |<---------------------------|                              |
```

BankID Login (Mobile)

```
Mobile App                 Hono API                     BankID OIDC
  |                           |                              |
  |  GET /v1/auth/bankid/initiate?platform=mobile            |
  |--------------------------->|                              |
  |  { redirectUrl, state }    |                              |
  |<---------------------------|                              |
  |                            |                              |
  |  Open BankID in secure browser (expo-web-browser)         |
```

```
|---------------------------------------------------------->|
|                            |                              |
|  User authenticates with BankID                           |
|                            |                              |
|  Redirect to drop://auth/callback?code=&state=            |
|<----------------------------------------------------------|
|                            |                              |
|  POST /v1/auth/bankid/callback                            |
|  { code, state, platform }                                |
|--------------------------->|                              |
|                            |  1. Exchange code for tokens |
|                            |----------------------------->|
|                            |  { id_token }                |
|                            |<-----------------------------|
|                            |  2. Verify ID token (JWKS)   |
|                            |  3. Parse pid, verify age    |
|                            |  4. Find/create user         |
|                            |  5. Create session           |
|  { token, data }           |                              |
|<---------------------------|                              |
|                            |                              |
|  Store token in AsyncStorage                              |
```

User Creation

BankID login automatically creates user accounts:

1. **Parse pid** from BankID ID token (Norwegian national ID, 11 digits)
2. **Hash pid** with SHA-256 for storage (`national_id_hash` column)
3. **Check existing** user by `national_id_hash`
4. **If new:** Create user with:
   - `kyc_status = 'approved'` (BankID = verified identity)
   - `kyc_method = 'bankid'`
   - `auth_provider = 'bankid'`
   - `password_hash = 'EIDONLY'` (sentinel — no password auth)
5. **Age check:** Must be >= 18 (parsed from pid birthdate)

JWT Structure

Payload

```
interface JwtPayload {
  userId: string;   // e.g., "usr_a1b2c3d4e5f6g7h8"
  email: string;    // e.g., "usr_xxx@bankid.drop.local"
  role: string;     // "user" or "merchant"
}
```

Claims

Claim	Value
`exp`	Current time + 24h (web) / 7d (mobile)
`iat`	Current time
`iss`	`drop-api` (Hono) / none (Next.js)
`aud`	`drop` (Hono) / none (Next.js)

Session Revocation

1. **On login:** `sessions` record created with SHA-256 hash of JWT
2. **On each request:** Verify session not revoked + not expired
3. **On logout:** All user sessions marked `revoked = 1`

CSRF Protection

- **Web:** State parameter in BankID OIDC flow (stored in httpOnly cookie)
- **API:** Origin header validation against allowed origins
- **Mobile:** N/A (Bearer token, no cookies)

Rate Limiting

Endpoint	Limit
BankID initiate	10/min per IP
BankID callback	10/min per IP
Auth me/logout/refresh	No additional limit (auth required)

Authorization

Role-Based Access

Two roles: `user` and `merchant`.

Route	Auth	Role
GET /auth/bankid/initiate	None	-
POST /auth/bankid/callback	None	-
GET /auth/me	Required	Any
POST /auth/logout	Required	Any
POST /auth/refresh	Required	Any
POST /merchants/register	Required	Any (upgrades to merchant)
GET /merchants/dashboard	Required	Merchant

Deprecated Endpoints

These endpoints return **410 Gone**:

Endpoint	Replacement
`POST /auth/login`	BankID OIDC flow
`POST /auth/register`	Automatic via BankID login
`POST /auth/verify-otp`	Not needed (BankID replaces OTP)

Environment Variables

Required (Production)

```
BANKID_CLIENT_ID          # BankID OIDC client ID
BANKID_CLIENT_SECRET      # BankID OIDC client secret
BANKID_CALLBACK_URL       # Web callback URL (e.g.,
https://getdrop.no/api/auth/bankid/callback)
BANKID_CALLBACK_URL_MOBILE # Mobile deep link (e.g., drop://auth/callback)
JWT_SECRET                # JWT signing secret (min 32 chars)
```

Optional

```
BANKID_AUTHORIZE_URL      # Default: BankID prod authorize endpoint
BANKID_TOKEN_URL          # Default: BankID prod token endpoint
BANKID_JWKS_URL           # Default: BankID prod JWKS endpoint
BANKID_ISSUER             # Default: BankID prod issuer
BANKID_MOCK=true          # Dev mode: mock OIDC flow (no real BankID needed)
JWT_ALGORITHM             # "HS256" (default) or "RS256"
JWT_EXPIRY                # Default: "24h"
```

Merchant Flow

Merchants use the same BankID login as regular users. After logging in:

1. Navigate to merchant registration
2. Fill in business details (business name, org number, bank account)
3. `POST /merchants/register` with auth token
4. User role upgraded from `user` to `merchant`
5. Merchant dashboard becomes accessible

Revision #12
Created 2026-02-18 08:44:21 UTC by John
Updated 2026-06-27 21:54:06 UTC by John