Market Research

- Mobile Banking Research
- Banking Providers
- MVP Specification
- Cost Analysis
- Technology Stack
- BankID & Vipps Research
- Cloud Cost Analysis

Mobile Banking Research

Mobile Payment/Banking Application - Full Research Findings

Table of Contents

1. Regulatory Requirements
2. Technical Architecture
3. Security & Compliance
4. Market Analysis
5. Key Success Factors

---

1. Regulatory Requirements

1.1 EU Payment Services Directive (PSD2/PSD3)

Current State (PSD2)

PSD2 has been the governing framework since 2018, establishing:

- Strong Customer Authentication (SCA) requirements
- Open Banking mandates for API access
- Liability frameworks for unauthorized transactions
- Consumer protection standards

PSD3 Transition (2025-2028)

Timeline:

- Political agreement reached: November 2025
- Formal adoption expected: Early-Mid 2026
- Transition period: 18-24 months after adoption
- Full compliance deadline: 2027-2028

Key Changes in PSD3:

- **Payment Services Regulation (PSR)**: Directly applicable across EU (no local transposition needed)
- **Enhanced SCA**: Stronger identity verification, tighter exemption management
- **Fraud Prevention**: Banks liable for certain impersonation scams, mandatory "Confirmation of Payee"
- **Expanded Scope**: Covers instant payments, BNPL, cryptocurrencies, digital identity
- **API Standards**: Improved technical and performance standards for Open Banking

Compliance Actions for 2026:

1. Implement Confirmation of Payee systems
2. Upgrade SCA mechanisms for eIDAS 2.0 alignment
3. Establish real-time fraud monitoring
4. Prepare for API hardening requirements
5. Build recovery assurance capabilities

1.2 Licensing Requirements

Electronic Money Institution (EMI) License

Capital Requirements:

- Full EMI: EUR 350,000 minimum capital (must be unencumbered)
- Small EMI: Available if < EUR 5M in outstanding e-money
  - Lower requirements
  - Application fee: EUR 1,000
  - Limited to home country (no passporting)

Application Costs by Jurisdiction:

Country	Application Fee	Timeline	Total Setup Cost
Lithuania	EUR 1,463	6-9 months	EUR 30K-50K
Malta	EUR 2,000-5,000	~6 months	EUR 40K-60K
Ireland	GBP 5,000	12-18 months	EUR 200K-300K+
UK	GBP 5,000	6-12 months	EUR 100K-200K

Lithuania Advantages:

- Fastest processing in EU (6-9 months)
- Strong fintech ecosystem (Revolut HQ)
- Government investment in fintech infrastructure
- Lower operational costs
- Full EU passporting rights

Ireland Advantages:

- Higher institutional credibility
- Better for UK/US partnerships
- Stronger for institutional clients
- More stringent = higher trust

Payment Institution (PI) License

Alternative to EMI if not issuing e-money:

- Lower capital requirement (EUR 20K-125K depending on services)
- Faster approval process
- Limited to payment services only

1.3 KYC/AML Requirements

EU AML Package 2025

New Framework:

- Anti-Money Laundering Authority (AMLA) operational late 2025
- EU Single Rulebook for harmonized requirements
- Direct supervision of selected entities from 2028

Core KYC Requirements:

1. **Customer Due Diligence (CDD)**
   - Identity verification (ID document + biometric)
   - Address verification
   - Source of funds verification
   - Beneficial ownership identification (UBO)
2. **Enhanced Due Diligence (EDD)**
   - Required for high-risk customers/transactions
   - PEP (Politically Exposed Persons) screening
   - Ongoing monitoring requirements
3. **eKYC Standards (2025)**
   - Mandatory electronic identification

- eIDAS 2.0 compliance for digital identity
- Remote verification capabilities required

Cash Transaction Limits:

- EU-wide cap: EUR 10,000 for cash payments
- Applies to all businesses dealing in high-value goods

1.4 Data Protection (GDPR)

Key Requirements for Financial Apps:

1. **Data Minimization**
   - Collect only necessary data
   - Clear purpose limitation
   - Defined retention periods
2. **Privacy by Default**
   - Location tracking disabled by default
   - Marketing communications opt-in only
   - Minimal data sharing defaults
3. **Consent Management**
   - Explicit, active consent required
   - No pre-ticked boxes
   - Easy withdrawal mechanism
   - Granular consent options
4. **Data Subject Rights**
   - Right to access (30-day response)
   - Right to portability
   - Right to erasure
   - Right to rectification
5. **Security Requirements**
   - End-to-end encryption (TLS 1.3+)
   - AES-256 for data at rest
   - Data breach notification within 72 hours
6. **DPIA Requirements**
   - Required for AI-powered decisions
   - Biometric authentication systems
   - Large-scale customer analytics

Penalties:

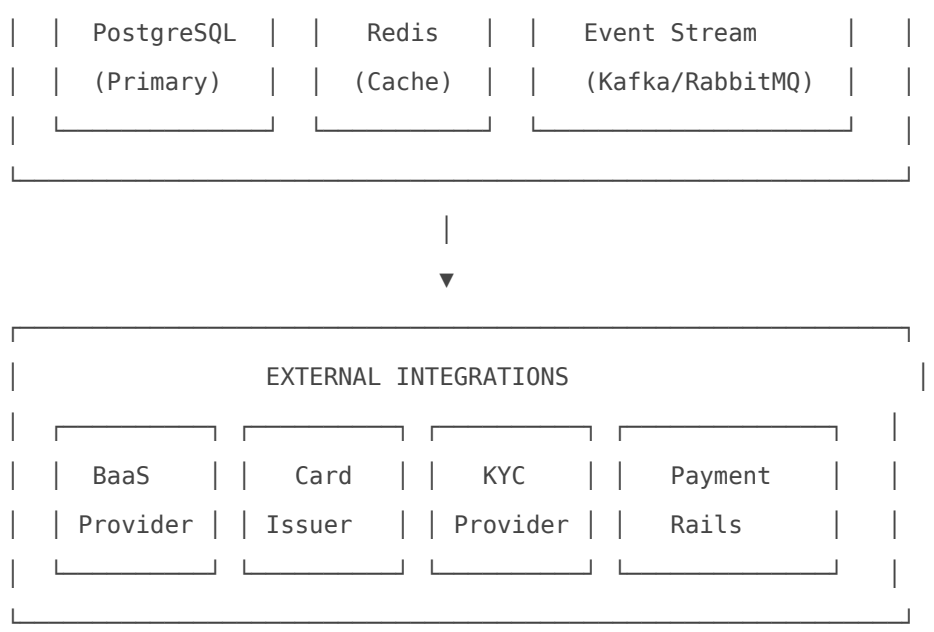
- Up to EUR 20 million or 4% of global annual turnover

---

2. Technical Architecture

2.1 System Architecture Overview

Modern mobile banking requires a **layered, microservices-based architecture**:



2.2 Payment Processing Flow

```
1. User Initiates Payment
         |
         ▼
2. Mobile App → API Gateway
         |
         ▼
3. Authentication Service (verify session, 2FA if required)
         |
         ▼
4. Payment Service
   ├── Validate request
   ├── Check balance/limits
   ├── AML screening (real-time)
   └── Create payment intent
         |
         ▼
5. Ledger Service
   ├── Reserve funds (pending state)
   └── Create audit trail
         |
         ▼
6. External Payment Rail (SEPA, SWIFT, card network)
         |
```

```
        ▼
7. Confirmation
   ├── Ledger finalization
   ├── User notification
   └── Transaction record
```

2.3 Mobile Wallet Architecture

Core Components:

1. **Wallet Container**
   - Multi-currency support
   - Real-time balance tracking
   - Transaction history
   - Spending analytics
2. **Card Management**
   - Virtual card generation
   - Physical card ordering
   - Card controls (freeze, limits)
   - Push provisioning (Apple/Google Pay)
3. **Payment Methods**
   - NFC tap-to-pay
   - QR code payments
   - P2P transfers
   - Scheduled payments
   - Bill payments
4. **Security Layer**
   - Biometric authentication
   - Device binding
   - Transaction signing
   - Tokenization

2.4 Core Banking Integration Options

Option 1: Full BaaS

- Use provider's complete stack
- Fastest time to market
- Limited customization
- Higher per-transaction costs

Option 2: Modular Integration

- Core banking from BaaS

- Own card program
- Custom payment rails
- Balanced approach

Option 3: Custom Build

- Own core banking system
- Maximum flexibility
- Highest development cost
- Longest timeline

2.5 API-First Design Principles

1. **RESTful APIs** for standard operations
2. **WebSocket** for real-time updates
3. **GraphQL** for complex data queries (optional)
4. **Idempotency** for payment operations
5. **Versioning** for backward compatibility
6. **Rate limiting** for security and stability

---

3. Security & Compliance

3.1 PCI DSS Compliance

Compliance Levels:

- Level 1: >6M transactions/year (QSA audit required)
- Level 2: 1-6M transactions/year
- Level 3: 20K-1M transactions/year
- Level 4: <20K transactions/year (self-assessment)

Key Requirements (v4.0.1):

Requirement	Description
Req 3	Protect stored cardholder data
Req 4	Encrypt transmission of cardholder data
Req 6	Develop and maintain secure systems
Req 8	Identify users and authenticate access
Req 10	Log and monitor all access

Requirement	Description
Req 11	Regularly test security systems
Req 12	Maintain information security policy

Mobile-Specific Requirements:

- Runtime Application Self-Protection (RASP)
- Code obfuscation
- White-box cryptography
- Secure key management
- Certificate pinning

Non-Compliance Penalties:

- EUR 5,000 - 100,000 per month
- Increased transaction fees
- Loss of payment processing capability

3.2 Strong Customer Authentication (SCA)

Two of Three Factors Required:

1. **Knowledge**: PIN, password
2. **Possession**: Phone, token, card
3. **Inherence**: Biometrics (fingerprint, face)

SCA Exemptions:

- Low-value transactions (<EUR 30)
- Recurring payments (same amount, same merchant)
- Trusted beneficiaries
- Low-risk transactions (based on fraud analysis)

3.3 Security Architecture

```
┌─────────────────────────────────────────────────┐
│              SECURITY LAYERS                    │
├─────────────────────────────────────────────────┤
│ Application Security                            │
│ ├── Input validation                            │
│ ├── Output encoding                             │
│ ├── Session management                          │
```

```
│ └── OWASP MASVS compliance                          │
├──────────────────────────────────────────────────────┤
│ Data Security                                        │
│ ├── AES-256 encryption (at rest)                     │
│ ├── TLS 1.3 (in transit)                             │
│ ├── Tokenization (sensitive data)                    │
│ └── Key management (HSM)                             │
├──────────────────────────────────────────────────────┤
│ Infrastructure Security                              │
│ ├── WAF (Web Application Firewall)                   │
│ ├── DDoS protection                                  │
│ ├── Network segmentation                             │
│ └── Intrusion detection                              │
├──────────────────────────────────────────────────────┤
│ Operational Security                                 │
│ ├── 24/7 monitoring                                  │
│ ├── Incident response                                │
│ ├── Penetration testing                              │
│ └── Vulnerability management                         │
└──────────────────────────────────────────────────────┘
```

3.4 Fraud Prevention

Real-Time Monitoring:

- Transaction velocity checks
- Geographic anomaly detection
- Device fingerprinting
- Behavioral biometrics
- ML-based risk scoring

Required Capabilities (PSD3):

- Confirmation of Payee (name matching)
- Real-time fraud data sharing between PSPs
- Impersonation scam detection
- Social engineering prevention

---

4. Market Analysis

4.1 European Digital Banking Market

Market Size:

- Digital banking users: 500M+ in Europe
- Mobile banking penetration: 70%+ in Western Europe
- Neobank market share growing at 25%+ annually

Key Players:

- Revolut (35M+ users)
- N26 (8M+ users)
- Monzo (9M+ users, UK)
- Bunq (12M+ users)

4.2 Competitive Landscape

Neobank Industry Statistics (2025):

- 76% of neobanks remain unprofitable
- Only 18% projected to break even by 2025
- Customer acquisition costs remain high
- Revenue diversification is key to profitability

Success Factors:

1. Differentiated value proposition
2. Superior user experience
3. Cost-efficient operations
4. Multiple revenue streams
5. Strong unit economics

4.3 Revenue Models

Primary Revenue Streams:

1. **Interchange fees**: 0.2-0.3% of card transactions
2. **FX markup**: 0.5-2% on currency conversion
3. **Subscription tiers**: EUR 5-15/month premium plans
4. **Interest income**: On deposits (if banking license)
5. **Lending**: Personal loans, BNPL, overdrafts

Emerging Revenue:

- Insurance products

- Investment/trading fees
- Business accounts (higher margins)
- Crypto services

---

5. Key Success Factors

5.1 Time to Market

Critical Milestones:

1. **Month 1-3**: Legal structure, licensing strategy
2. **Month 3-6**: BaaS integration, MVP development
3. **Month 6-9**: Beta testing, compliance audit
4. **Month 9-12**: Public launch, scaling

Accelerators:

- Use BaaS provider (vs. own license initially)
- Cross-platform mobile development
- Pre-built KYC/AML integrations
- Cloud-native infrastructure

5.2 User Acquisition

Strategies:

1. **Referral programs**: Proven effective for neobanks
2. **Niche targeting**: Specific customer segments
3. **Feature differentiation**: Unique value proposition
4. **Partnership distribution**: Through platforms/employers

Metrics to Track:

- Customer Acquisition Cost (CAC)
- Lifetime Value (LTV)
- LTV:CAC ratio (target >3:1)
- Activation rate (target >25%)
- Monthly active users (MAU)

5.3 Operational Excellence

Key Capabilities:

1. **Customer support**: 24/7, multi-channel
2. **Fraud management**: Real-time, ML-powered
3. **Compliance**: Continuous monitoring
4. **Engineering**: Rapid iteration, reliability

Cost Optimization:

- AI chatbots (reduce support costs 60%)
- Automated KYC (reduce onboarding costs)
- Cloud-native (elastic scaling)
- Outsourced development (40-60% savings)

Sources and References

Regulatory

- PSD3 & PSR Overview - Flagright
- PSD3 - J.P. Morgan
- EMI License Guide - InnReg
- AML 2025 - Moody's
- GDPR for Financial Services - InnReg

Technical

- Mobile Banking Architecture - Crassula
- Digital Wallet Guide 2025 - Scalefocus
- PCI DSS Mobile App Compliance - Promon
- Mobile Banking App Development - Leanware

Market

- Neobank Industry Statistics 2025 - Coinlaw
- BaaS Market Overview - FinTech Magazine
- Digital Wallet Development - ITU Technical Report

Banking Providers

Third-Party Providers Comparison

> **Architecture alignment note (2026-02-14):** This document is pre-architecture research from the mobilebank-research phase. Drop ultimately chose a **PSD2 pass-through model** — no wallet, no balance held by Drop, no IBAN generation. BaaS providers listed here would serve as Open Banking (AISP/PISP) integration partners, not wallet infrastructure. Card issuing is a FUTURE feature (feature-flagged). This document is retained as provider research reference.

Table of Contents

1. Banking-as-a-Service (BaaS) Providers
2. Card Issuing Platforms
3. Payment Processors
4. KYC/Identity Verification Providers
5. Virtual IBAN Providers
6. Recommendation Matrix

---

1. Banking-as-a-Service (BaaS) Providers

Overview

BaaS providers enable fintech companies to offer banking services without obtaining their own banking license. They provide the regulatory infrastructure, APIs, and banking capabilities.

Provider Comparison

Solarisbank (Solaris SE)

Attribute	Details
Headquarters	Berlin, Germany
License	Full German banking license + Digital Assets Custody
Coverage	EU-wide (passporting)
Key Features	Accounts, cards, lending, digital assets, compliance
Target Market	Fintechs, enterprises, large card programs
Notable Clients	Samsung, ADAC
Strengths	Full-stack, modular APIs, banking license
Weaknesses	Requires BaFin approval for new partners, financial challenges
Best For	Enterprises needing complete banking capabilities

Services:

- Current accounts with IBAN
- Card issuing (virtual + physical)
- Lending products
- Digital asset custody
- Full compliance stack

Swan

Attribute	Details
Headquarters	Paris, France
License	EMI (French)
Coverage	Eurozone (expanding)
Key Features	IBANs, cards, embedded finance
Target Market	Startups, SMEs, SaaS platforms
Strengths	5-minute integration, built-in KYC, fast time-to-market
Weaknesses	Limited geographic coverage, cards/accounts focus

Attribute	Details
Best For	Fast MVP launch, European startups

Key Differentiators:

- Claims 10X shorter implementation time
- KYC/fraud detection built into product (no extra cost)
- Developer-friendly APIs
- Good for expense management, HR tech, proptech

Treezor (Societe Generale)

Attribute	Details
Headquarters	Paris, France
License	EMI (European) + MasterCard Prepaid approved
Coverage	EU (branches in Italy, Spain, Germany)
Key Features	E-wallets, cards, marketplaces, crowdfunding
Target Market	Neobanks, mobility, employee benefits
Strengths	Backed by Societe Generale, SEPA network, 50M+ transactions/year
Weaknesses	Best suited for eurozone transactions
Best For	Euro-focused operations, established platforms

Services:

- White-label prepaid cards
- E-wallets
- Marketplace payments
- Crowdfunding solutions

Railsr (formerly Railsbank)

Attribute	Details
Headquarters	UK
License	EMI
Coverage	Europe, Asia
Key Features	BaaS, Cards-as-a-Service, payments, compliance
Target Market	Fintechs, brands embedding finance

Attribute	Details
Strengths	Flexible APIs, cards + payments combined
Weaknesses	Financial challenges (acquired/recapitalized 2023)
Best For	Card programs, embedded finance for brands

Other Notable Providers

Provider	HQ	Specialty	Notes
Modulr	UK	Payments infrastructure	EMI license, fast payments
Paynetics	Bulgaria	E-money, cards	EU + UK licenses
Vodeno/Aion	Poland/Belgium	Full banking	Acquired by UniCredit
OpenPayd	UK	Multi-currency accounts	Virtual IBANs specialist

BaaS Selection Criteria

1. **Regulatory Coverage**: Does license cover target markets?
2. **API Quality**: Developer documentation, SDKs, sandbox
3. **Time to Market**: Integration complexity, onboarding time
4. **Pricing Model**: Setup fees, per-transaction, revenue share
5. **Financial Stability**: Provider's funding, profitability
6. **Scalability**: Can grow with your business
7. **Support**: Technical support, account management

---

2. Card Issuing Platforms

Provider Comparison

Marqeta

Attribute	Details
Headquarters	US (global coverage)
Coverage	40+ countries
Key Features	Virtual/physical cards, JIT funding, customization
PCI Compliance	Level 1, tokenization
Pricing	~$0.50/virtual card, 0.5-1% transaction fee

Attribute	Details
Setup Cost	$5,000-$50,000
Best For	Custom card programs, expense management

Strengths:

- Open API architecture
- Just-in-Time (JIT) funding
- Real-time transaction control
- Extensive customization options

Stripe Issuing

Attribute	Details
Headquarters	US (Ireland for EU)
Coverage	US, EU expanding
Key Features	Virtual/physical cards, webhooks, Stripe ecosystem
Integration	Seamless with Stripe payments
Best For	Existing Stripe users, developer-centric teams

Strengths:

- Real-time authorization hooks
- PCI compliance handled by Stripe
- Apple Pay / Google Pay integration
- Excellent developer experience

Adyen Issuing

Attribute	Details
Headquarters	Netherlands
Coverage	Global
Key Features	Issuing + acquiring + processing combined
Integration	Single API for all payment needs
Best For	Enterprise with complex payment needs

Strengths:

- Unified platform (issuing + acquiring)

- 3D Secure built-in
- Real-time reporting
- Global compliance (GDPR, PSD2)

Other Card Issuers

Provider	Specialty	Coverage
Paymentology	Cloud-based issuing	Global
Thredd (GPS)	Prepaid programs	EU, UK
Wallester	European cards	EU
Galileo	Processing platform	US, expanding

---

3. Payment Processors

Adyen

Attribute	Details
Pricing Model	Interchange++ (most transparent)
Processing Fee	EUR 0.10-0.15 per transaction
Interchange	Pass-through (EU capped: 0.2% debit, 0.3% credit)
Payment Methods	Cards, local methods, wallets
Best For	Large volume, international operations

Strengths:

- Direct connections to card networks
- Local payment methods (SEPA, iDEAL, etc.)
- Single platform for global payments
- 50% EBITDA margin (financially stable)

Stripe

Attribute	Details
Pricing	1.4% + EUR 0.25 (EU cards), 2.9% + EUR 0.25 (non-EU)
Features	Payments, subscriptions, connect, treasury
Best For	Startups, developer-first companies

Strengths:

- Excellent documentation
- Rapid integration
- Broad feature set (payments, issuing, treasury)
- Strong developer community

Stripe Treasury (Embedded Finance)

Feature	Capability
Financial Accounts	Stored-value accounts for customers
Bank Integration	Fifth Third Bank partnership
FDIC Insurance	Pass-through eligible
ACH/Wire	Supported
Use Case	Embedded banking for platforms

Notable Implementation: Shopify Balance built on Stripe Treasury

---

Other Payment Processors

Provider	Specialty	Pricing Model
Checkout.com	Enterprise payments	Interchange++
Mollie	European SMB	Fixed % per method
Worldpay	Global acquiring	Custom
PayPal/Braintree	Consumer payments	Fixed %

---

4. KYC/Identity Verification Providers

Provider Comparison

Onfido

Attribute	Details
Services	ID scanning, facial recognition, risk scoring
Coverage	Global (195+ countries)

Attribute	Details
Integration	SDK (iOS, Android, Web) + API
Compliance	GDPR, eIDAS, SOC 2
Best For	High-volume onboarding, international

Sumsub

Attribute	Details
Services	KYC, AML screening, fraud prevention
Coverage	220+ countries
Features	Bank verification, PEP/sanctions screening
Best For	Growing fintechs, multi-region expansion

IDnow

Attribute	Details
Services	Video-based verification, eIDAS compliance
Coverage	Europe focus
Compliance	BaFin approved, full eIDAS
Best For	German market, strict compliance requirements

Entrust

Attribute	Details
Recognition	Gartner Magic Quadrant 2025
Services	AI-powered verification, digital onboarding
Best For	Enterprise, banking institutions

Comparison Matrix

Provider	Document Types	Biometrics	AML Screening	Pricing Range
Onfido	4,500+	Face match	Yes	$$$
Sumsub	3,000+	Face + liveness	Yes	$$
IDnow	EU focus	Video + face	Yes	$$$
Ondato	2,000+	Photo/video	Yes	$$

Provider	Document Types	Biometrics	AML Screening	Pricing Range
Trulioo	Global databases	Limited	Yes	$$
iDenfy	3,000+	Face + liveness	Yes	$

5. Virtual IBAN Providers

Key Providers

OpenPayd

Attribute	Details
IBAN Countries	UK, FR, MT, NL
Features	Named vIBANs, Target2 connectivity
API	Simple (2 required params)
Best For	Platforms needing named accounts

Banking Circle

Attribute	Details
Headquarters	Luxembourg
Features	Named vIBANs, multi-currency (EUR, GBP, USD, AED)
Target	High-volume PSPs, EMIs

Airwallex

Attribute	Details
Coverage	60+ markets
Features	Global accounts, FX, API automation
Best For	International operations

Other Providers

Provider	Specialty

Payset	SME-focused, multi-currency
Clear Junction	High-risk friendly
Currencycloud	FX + accounts
Sharpay	Instant issuance, SEPA/SWIFT

IBAN Provider Selection Criteria

1. **Coverage**: Which IBAN countries needed?
2. **Naming**: Named vs. pooled IBANs
3. **Payment Rails**: SEPA, SWIFT, Target2
4. **Currency Support**: EUR, GBP, USD, others
5. **API Quality**: Documentation, reliability
6. **Compliance**: AML/KYC support
7. **Pricing**: Per-account, per-transaction fees

---

6. Recommendation Matrix

By Company Stage

Stage	BaaS	Cards	KYC	Payments
MVP/Seed	Swan	Stripe Issuing	Sumsub	Stripe
Growth	Treezor/Railsr	Marqeta	Onfido	Adyen
Enterprise	Solarisbank	Marqeta/Adyen	IDnow	Adyen

By Use Case

Use Case	Recommended Stack
B2C Neobank	Solarisbank + Marqeta + Onfido
B2B Expense	Swan + Stripe Issuing + Sumsub
Marketplace	Treezor + Stripe + Ondato
Remittance	OpenPayd + Wise API + Trulioo
Embedded Finance	Stripe Treasury + Stripe Issuing + Sumsub

By Budget

Budget	Recommended Approach
< EUR 100K	Swan/Stripe ecosystem, Sumsub, minimal custom
EUR 100-500K	BaaS + card issuer + KYC stack
EUR 500K+	Full custom integration, enterprise providers

Sources

- Top BaaS Providers - FinTech Magazine
- BaaS Providers 2025 - SDK.finance
- Card Issuing APIs - Marqeta
- Virtual Card APIs 2025 - Buvei
- KYC Providers 2025 - Ondato
- Virtual IBAN Providers - SDK.finance
- Adyen Pricing - Finexer
- Stripe Treasury - Stripe Documentation

MVP Specification

MVP Feature Specification

> **Architecture alignment note (2026-02-14):** This document is pre-architecture research from the mobilebank-research phase. Drop ultimately chose a **PSD2 pass-through model** — no wallet, no balance held, no IBAN generation, no top-up. AISP reads bank balances, PISP initiates payments from the user's own bank account. Cards are a FUTURE feature (feature-flagged). This document is retained as research reference — it does NOT reflect the current Drop architecture.

Table of Contents

1. MVP Philosophy
2. Core Features
3. Feature Specifications
4. Timeline
5. Success Metrics

---

1. MVP Philosophy

Focus Areas

- **89% of user retention** comes from 5 key features (Gartner 2025)
- 3-minute onboarding is critical (74% abandon if >5 minutes)
- Avoid low-impact features (68% ignore crypto/loans in MVP)

What to Include

- Account creation and KYC

- IBAN generation
- Card issuing (virtual)
- P2P transfers
- Basic top-up

What to Exclude (MVP)

- Crypto trading
- Loan products
- Investment features
- Advanced analytics

---

2. Core Features

Feature Priority Matrix

Feature	Priority	Complexity	Timeline
User Onboarding	P0	Medium	Week 1-4
Digital KYC	P0	High	Week 2-6
Account Creation	P0	Medium	Week 4-8
IBAN Generation	P0	Low	Week 6-8
Virtual Card	P0	High	Week 8-12
P2P Transfers	P0	Medium	Week 10-14
Top-up (Card)	P1	Medium	Week 12-16
Bank Transfer	P1	Medium	Week 14-18
Transaction History	P1	Low	Week 8-10
Push Notifications	P1	Low	Week 10-12
Physical Card	P2	High	Post-MVP

---

3. Feature Specifications

3.1 User Onboarding

Goal: Complete signup in <3 minutes

Flow:

1. Download app
2. Enter phone number
3. Verify via OTP
4. Enter email
5. Set password/PIN
6. Accept T&C
7. Start KYC

Requirements:

- Phone number validation
- OTP delivery (<30 sec)
- Email verification
- Password strength rules
- Biometric setup (optional)

Acceptance Criteria:

- 95% OTP delivery rate
- <3 min completion time
- > 25% activation rate

3.2 Digital KYC (Know Your Customer)

Goal: Verify identity in <5 minutes

Flow:

1. Select ID document type
2. Capture front of ID
3. Capture back of ID (if applicable)
4. Take selfie (liveness check)
5. Enter personal details
6. Verification processing
7. Result notification

Document Types:

- Passport

- National ID card
- Driving license (select countries)

Requirements:

- Document OCR
- Face matching (>98% accuracy)
- Liveness detection
- PEP/Sanctions screening
- Address verification (optional)

Integration: Sumsub or Onfido API

Acceptance Criteria:

- > “ 85% auto-approval rate

- <2 min average verification
- Manual review queue for failures

3.3 Account Creation

Goal: Generate EUR account with IBAN

Flow:

1. KYC approved
2. Account type selection (Personal)
3. IBAN generation
4. Account activated
5. Welcome notification

Account Features:

- Single EUR account (MVP)
- Real-time balance
- Account details view
- Statement generation (PDF)

Integration: BaaS provider (Swan/Treezor)

Acceptance Criteria:

- Instant IBAN generation

- Valid SEPA-reachable IBAN
- Real-time balance updates

3.4 IBAN Generation

Technical Requirements:

- Named virtual IBAN (user's name)
- SEPA reachable
- Target2 compatible (if available)
- Instant credit notification

Provider Options:

- BaaS provider native
- OpenPayd (if separate)
- Banking Circle

Formats:

- Display: XX00 0000 0000 0000 0000 00
- Copy to clipboard
- Share via QR code

3.5 Virtual Card Issuing

Goal: Instant virtual Mastercard/Visa

Features:

- Instant generation post-account
- Add to Apple Pay / Google Pay
- Card details view (PAN, CVV, expiry)
- Freeze/unfreeze toggle
- Spending limits
- Transaction notifications

Card Controls:

- Online payments: ON/OFF
- ATM withdrawals: ON/OFF (N/A virtual)
- Contactless: ON/OFF
- Geographic restrictions

Security:

- PCI DSS compliant display
- 3D Secure enabled
- Real-time fraud monitoring

Integration: Marqeta or Stripe Issuing

Acceptance Criteria:

- <10 sec card generation
- Successful wallet provisioning
- Real-time transaction auth

3.6 P2P Transfers

Goal: Send money to other users instantly

Transfer Types:

A) Internal (App-to-App)

- By phone number
- By username
- By QR code
- Instant settlement

B) SEPA Transfer

- By IBAN
- Standard SEPA (D+1)
- SEPA Instant (if available)

Flow:

1. Select recipient method
2. Enter/select recipient
3. Enter amount
4. Review details
5. Authenticate (biometric/PIN)
6. Confirmation

Requirements:

- Amount validation (balance check)

- Transaction limits
- Confirmation of Payee (name match)
- Audit trail

Limits (MVP):

Type	Daily	Monthly
Internal	EUR 5,000	EUR 20,000
SEPA	EUR 2,000	EUR 10,000

3.7 Top-up Methods

A) Card Top-up

- Visa/Mastercard debit/credit
- 3D Secure required
- Instant credit
- Fee: 1-2% (or included in premium)

B) Bank Transfer

- SEPA inbound to IBAN
- Auto-reconciliation
- Credit on receipt

C) Future: Apple Pay / Google Pay top-up

Integration: Stripe or Adyen for card payments

3.8 Transaction History

Features:

- Real-time updates
- Filter by type/date/amount
- Search functionality
- Transaction details
- Receipt/proof generation
- Export (CSV, PDF)

Categories:

- Card payments
- Transfers (in/out)
- Top-ups
- Fees

3.9 Push Notifications

Mandatory Notifications:

- Transaction alerts (all)
- Login from new device
- Card frozen/unfrozen
- KYC status updates
- Security alerts

Optional Notifications:

- Marketing
- Product updates
- Weekly spending summary

---

4. Timeline

Phase 1: Foundation (Months 1-2)

Week 1-4:

- Project setup, CI/CD
- BaaS integration start
- Auth service
- User onboarding flow

Week 5-8:

- KYC integration
- Account creation
- IBAN generation
- Basic app UI

Phase 2: Core Features (Months 3-4)

Week 9-12:

- Virtual card issuing
- Wallet provisioning
- Transaction history
- Push notifications

Week 13-16:

- P2P transfers (internal)
- Card top-up
- Basic card controls

Phase 3: Launch Prep (Months 5-6)

Week 17-20:

- SEPA transfers
- Bank transfer top-up
- Security hardening
- Compliance audit

Week 21-24:

- Beta testing (500 users)
- Bug fixes
- Performance optimization
- Soft launch

Milestones

Milestone	Target Date	Deliverable
Alpha	Month 3	Core features working
Beta	Month 5	500 beta users
Soft Launch	Month 6	Public availability
GA	Month 7-8	Marketing push

---

5. Success Metrics

Activation Metrics

Metric	Target	Threshold
Signup completion	>80%	>60%
KYC pass rate	>85%	>70%
First transaction	>50% in 7 days	>30%
Card activation	>70%	>50%

Engagement Metrics

Metric	Target	Threshold
MAU/DAU	>30%	>20%
Transactions/user/month	>10	>5
App opens/week	>3	>1

Quality Metrics

Metric	Target	Threshold
App crash rate	<0.5%	<1%
API latency (p95)	<500ms	<1000ms
Uptime	>99.9%	>99.5%
App store rating	>4.5	>4.0

Business Metrics

Metric	Target	Threshold
CAC	<EUR 30	<EUR 50
Monthly burn	<EUR 50K	<EUR 75K
Active users (6 months)	>5,000	>2,000

Sources

- Neobank MVP Guide - Designography

- How to Start a Neobank - DashDevs
- Mobile Wallet Features - SDK.finance
- Neobank Development - 4IRE Labs

Cost Analysis

Cost Breakdown and Budget Estimates

> **Architecture alignment note (2026-02-14):** This document is pre-architecture research from the mobilebank-research phase. Drop ultimately chose a **PSD2 pass-through model** — no wallet, no balance held, no own EMI license required for MVP. The pass-through model significantly reduces licensing and BaaS costs compared to the scenarios below. Card issuing is a FUTURE feature. This document is retained as cost research reference — actual Drop cost structure differs.

Table of Contents

1. Executive Summary
2. Licensing Costs
3. Development Costs
4. Third-Party Provider Costs
5. Infrastructure Costs
6. Operational Costs
7. Budget Scenarios

---

1. Executive Summary

Total Investment Range

Approach	Initial (Year 1)	Monthly Ops	Break-even

BaaS MVP	EUR 150K-300K	EUR 15-30K	18-24 months
Full Build	EUR 500K-1.5M	EUR 50-100K	24-36 months
Enterprise	EUR 1.5M+	EUR 100K+	36+ months

Key Cost Drivers

1. Licensing strategy (own vs. BaaS)
2. Development approach (in-house vs. outsource)
3. Feature complexity
4. Geographic scope
5. Transaction volume

---

2. Licensing Costs

Option A: Own EMI License

Jurisdiction	Application	Capital	Setup (Legal/Consulting)	Timeline
Lithuania	EUR 1,463	EUR 350,000	EUR 30-50K	6-9 months
Malta	EUR 2-5K	EUR 350,000	EUR 40-60K	6 months
Ireland	EUR 4K	EUR 350,000	EUR 200-300K	12-18 months
UK (FCA)	GBP 5,000	GBP 350,000	GBP 100-200K	6-12 months

Lithuania Breakdown:

- Application fee: EUR 1,463
- Capital requirement: EUR 350,000 (held in local bank)
- Legal/consulting: EUR 30,000-50,000
- Directors/compliance staff: EUR 100,000+/year
- **Total setup: ~EUR 400,000-500,000**

Option B: BaaS Partnership (No Own License)

Provider	Setup Fee	Monthly Minimum	Per-Transaction
Swan	EUR 0-10K	EUR 500-2K	Volume-based
Treezor	EUR 10-50K	EUR 2-5K	Volume-based
Solarisbank	EUR 50-100K	EUR 5-10K	Custom

Savings with BaaS:

- No EUR 350K capital lock-up
- No license application process
- Faster time to market (weeks vs. months)
- Compliance handled by provider

---

3. Development Costs

MVP Development (4-6 months)

Component	In-House (Western EU)	Outsource (Eastern EU)	Outsource (Asia)
Backend	EUR 80-120K	EUR 40-60K	EUR 25-40K
Mobile (Flutter)	EUR 60-100K	EUR 30-50K	EUR 20-35K
Frontend (Web)	EUR 30-50K	EUR 15-25K	EUR 10-18K
DevOps/Infra	EUR 20-40K	EUR 10-20K	EUR 8-15K
QA/Testing	EUR 20-30K	EUR 10-15K	EUR 6-10K
Total	**EUR 210-340K**	**EUR 105-170K**	**EUR 69-118K**

Feature-Level Costs

Feature	Development Cost	Notes
User onboarding	EUR 8-15K	Auth, registration
KYC integration	EUR 15-30K	Third-party API
Account management	EUR 20-35K	Core functionality
Virtual card	EUR 25-40K	Issuing integration
P2P transfers	EUR 15-25K	Internal + SEPA
Card top-up	EUR 10-20K	Payment gateway
Push notifications	EUR 5-10K	FCM/APNS
Transaction history	EUR 8-12K	UI + backend
Card controls	EUR 10-15K	Freeze, limits

Team Composition (MVP)

Role	Count	Monthly Cost (EU)
Tech Lead	1	EUR 8-12K
Backend Dev (Senior)	2	EUR 12-18K
Mobile Dev (Senior)	2	EUR 12-18K
DevOps	1	EUR 6-9K
QA	1	EUR 4-6K
Product Manager	1	EUR 6-10K
Designer	0.5	EUR 3-5K
Total	**8.5**	**EUR 51-78K/month**

Outsourcing Savings: 40-60% vs. Western EU rates

---

4. Third-Party Provider Costs

BaaS Provider Costs

Provider	Setup	Monthly	Per Account	Notes
Swan	Free-10K	EUR 500-2K	EUR 0.50-2	Fast integration
Treezor	EUR 10-30K	EUR 2-5K	Included	SEPA optimized
Solarisbank	EUR 50-100K	EUR 5-10K	Custom	Full stack

Card Issuing Costs

Provider	Setup	Per Card	Transaction Fee
Marqeta	EUR 5-50K	EUR 0.50-2	0.5-1%
Stripe Issuing	Free	EUR 0.10-0.50	Included
Adyen	Custom	Custom	Custom

KYC/Identity Verification

Provider	Per Verification	Volume Discount
Sumsub	EUR 0.50-2.00	Yes (>10K/month)
Onfido	EUR 1.00-3.00	Yes

Provider	Per Verification	Volume Discount
IDnow	EUR 2.00-5.00	Yes

Example (10K users/month):

- Sumsub: EUR 5,000-20,000/month
- Volume pricing reduces to EUR 0.30-0.50/verification

Payment Processing

Provider	Setup	Per Transaction	Notes
Stripe	Free	1.4% + EUR 0.25 (EU)	Easy integration
Adyen	Free	EUR 0.10-0.15 + interchange	Enterprise

Virtual IBAN

Provider	Per IBAN	Monthly Maintenance
OpenPayd	EUR 1-5	EUR 0-1
Banking Circle	Custom	Volume-based
Usually included in BaaS	-	-

---

5. Infrastructure Costs

Cloud Infrastructure (AWS/GCP)

Component	Monthly Cost	Notes
Compute (K8s cluster)	EUR 1,500-3,000	3-5 nodes
Database (RDS/Cloud SQL)	EUR 500-1,500	Multi-AZ
Redis (ElastiCache)	EUR 200-500	Cluster mode
Storage (S3)	EUR 100-300	Documents, backups
CDN (CloudFlare)	EUR 200-500	Pro/Business
Monitoring (Datadog)	EUR 300-800	APM included
Total	**EUR 2,800-6,600**	Scales with users

Cost Per User

Users	Infrastructure	Third-Party	Total/User
1,000	EUR 3/user	EUR 5/user	EUR 8/user
10,000	EUR 1/user	EUR 3/user	EUR 4/user
100,000	EUR 0.50/user	EUR 2/user	EUR 2.50/user

---

6. Operational Costs

Monthly Operational Expenses

Category	MVP Phase	Growth Phase	Scale Phase
Team (salaries)	EUR 30-50K	EUR 80-150K	EUR 200K+
Infrastructure	EUR 3-5K	EUR 10-20K	EUR 50K+
Third-party services	EUR 5-10K	EUR 20-50K	EUR 100K+
Compliance	EUR 5-10K	EUR 15-30K	EUR 50K+
Customer support	EUR 2-5K	EUR 10-20K	EUR 30K+
Marketing	EUR 5-15K	EUR 30-100K	EUR 200K+
Legal/Professional	EUR 2-5K	EUR 5-15K	EUR 20K+
Office/Admin	EUR 2-5K	EUR 5-10K	EUR 15K+
Total	**EUR 54-105K**	**EUR 175-395K**	**EUR 665K+**

Per-User Economics

Metric	Amount	Notes
Customer Acquisition Cost	EUR 20-50	Marketing + onboarding
First-year serving cost	EUR 175	Fixed costs
Monthly serving cost	EUR 5	Infrastructure + support
Required spend for breakeven	EUR 750/month	Year 1

Compliance Costs

Item	Annual Cost
Compliance Officer (FTE)	EUR 80-120K
AML monitoring tools	EUR 20-50K
External audits	EUR 30-60K
Regulatory reporting	EUR 10-20K
Training & certification	EUR 5-10K
Total	**EUR 145-260K**

---

7. Budget Scenarios

Scenario A: Lean BaaS MVP

Assumptions:

- BaaS partnership (Swan)
- Outsourced development (Eastern EU)
- 6-month timeline
- Target: 5,000 users Year 1

Category	Year 1	Monthly (Avg)
Development	EUR 150,000	-
BaaS setup + fees	EUR 20,000	EUR 2,000
KYC (5K verifications)	EUR 10,000	EUR 1,000
Infrastructure	EUR 36,000	EUR 3,000
Operations (lean)	EUR 120,000	EUR 10,000
Marketing	EUR 60,000	EUR 5,000
Legal/Compliance	EUR 30,000	EUR 2,500
Buffer (15%)	EUR 64,000	-
Total Year 1	**EUR 490,000**	**EUR 23,500**

Scenario B: Standard Build

Assumptions:

- Own EMI license (Lithuania)

- Mixed team (in-house + outsource)
- 12-month timeline
- Target: 20,000 users Year 1

Category	Year 1	Monthly (Avg)
EMI License	EUR 450,000	-
Development	EUR 300,000	-
Card program	EUR 50,000	EUR 5,000
KYC (20K verifications)	EUR 30,000	EUR 3,000
Infrastructure	EUR 72,000	EUR 6,000
Operations	EUR 480,000	EUR 40,000
Marketing	EUR 200,000	EUR 17,000
Legal/Compliance	EUR 150,000	EUR 12,500
Buffer (20%)	EUR 346,000	-
Total Year 1	**EUR 2,078,000**	**EUR 83,500**

Scenario C: Enterprise Launch

Assumptions:

- Own license (Ireland for prestige)
- Full in-house team
- Custom core banking
- Target: 100,000 users Year 1

Category	Year 1
EMI License (Ireland)	EUR 800,000
Development	EUR 800,000
Core banking platform	EUR 300,000
Card program	EUR 150,000
KYC (100K verifications)	EUR 100,000
Infrastructure	EUR 300,000
Operations	EUR 1,500,000
Marketing	EUR 1,000,000
Legal/Compliance	EUR 400,000
Buffer (25%)	EUR 1,337,500

Category	Year 1
Total Year 1	**EUR 6,687,500**

Cost Optimization Strategies

Development

- Outsource to Eastern EU (40-60% savings)
- Use BaaS to reduce custom development
- Cross-platform mobile (Flutter) vs. native

Licensing

- Start with BaaS, migrate to own license later
- Lithuania over Ireland (70% cheaper)
- Small EMI if eligible

Operations

- AI chatbots reduce support costs 60%
- Automated KYC reduces manual review
- Cloud-native for elastic scaling

Marketing

- Referral programs (lower CAC)
- Partnership distribution
- Niche targeting

Financial Model Summary

Unit Economics Target

Metric	Target
CAC	< EUR 30

Metric	Target
LTV	> EUR 150
LTV:CAC	> 5:1
Payback period	< 12 months
Gross margin	> 60%

Revenue Model

Stream	Revenue/User/Year
Interchange	EUR 15-30
FX markup	EUR 10-20
Premium subscription	EUR 60-120
Interest income	EUR 5-15
Total potential	**EUR 90-185**

Break-even Analysis

Scenario	Users Required	Timeline
BaaS MVP	5,000-10,000	18-24 months
Standard	20,000-30,000	24-36 months
Enterprise	50,000+	36+ months

Sources

- Neobank Development Cost - ITExus
- Banking App Development Cost - Leanware
- EMI License Costs - Tangle.ee
- Neobank Industry Statistics - Coinlaw
- Start a Neobank Guide - RND Point
- Adyen Pricing - Finexer

Technology Stack

Technical Stack Recommendations

1. Architecture Overview

Principles

1. **Microservices Architecture** - Modular, independently deployable
2. **Cloud-Native Design** - Containerized, elastic scaling
3. **Security by Design** - Zero-trust, encryption everywhere

2. Backend Technology

Primary: Java/Spring Boot

- Built-in Spring Security, OAuth2
- ACID compliance for transactions
- Proven in regulated industries
- Spring Boot 3.x, Spring Cloud

Secondary: Node.js

- WebSocket connections
- Push notifications
- Real-time updates

Hybrid Approach

- **Java**: Auth, Accounts, Payments, Cards, Ledger, KYC/AML
- **Node.js**: WebSocket, Notifications, Real-time

- **Python**: Fraud ML, Risk Scoring, Analytics

3. Mobile Development

Recommendation: Flutter

Criteria	Flutter	React Native	Native
Performance	Near-native	Good	Best
Code Sharing	95%+	85-90%	0%
Market Share	46%	35%	-

Why Flutter:

- Same UI across iOS/Android
- Single codebase
- No JS bridge
- Used by major banks

Stack: Bloc, GoRouter, Dio, Hive, local_auth

4. Database & Storage

- **Primary**: PostgreSQL 16
- **Cache**: Redis 7
- **Queue**: Kafka/RabbitMQ
- **Documents**: S3
- **Search**: Elasticsearch

5. Infrastructure

Cloud: AWS or GCP

Components:

- Kubernetes (EKS/GKE)
- Terraform
- GitHub Actions + ArgoCD

- Prometheus + Grafana
- CloudFlare (WAF)

6. Security

OWASP MASVS

- AES-256, TLS 1.3
- Biometric auth, 2FA
- Certificate pinning
- Code obfuscation

7. MVP Stack

- **Backend**: Java 21 + Spring Boot 3.2, Node.js 20
- **Mobile**: Flutter 3.x
- **Data**: PostgreSQL, Redis, Kafka
- **Infra**: AWS/GCP, K8s, Terraform
- **Third-Party**: Swan (BaaS), Stripe Issuing, Sumsub (KYC)

BankID & Vipps Research

BankID and Vipps Login Authentication Research

Research Date: 2026-02-15 **Project:** Drop Fintech App **Purpose:** Evaluate feasibility of integrating BankID and Vipps as authentication methods

---

Executive Summary

Both BankID and Vipps Login are viable authentication options for Drop. Both support OIDC/OAuth2 integration with Next.js, have test environments, and can serve dual purposes as both authentication and PSD2 Strong Customer Authentication (SCA).

Critical Timeline Note: BankID is undergoing major changes with an April 1, 2026 deadline for migration to new infrastructure.

Key Considerations:

- BankID requires Norwegian bank account and 10 business days for production access
- Vipps has lower per-transaction costs (DKK 0.00-0.40 vs DKK 0.65-0.89)
- Both services can be accessed via aggregators (Idura/Signicat) which simplify integration
- Both meet PSD2 SCA requirements

---

1. Norwegian BankID

What is it?

BankID is Norway's leading electronic identification system, issued through Norwegian banks. It enables secure authentication and digital signatures. BankID supports both traditional methods and the newer BankID with Biometrics (app-based solution using WebAuthn).

Major Change in 2026: BankID is moving to a single issuer (Stø AS) with critical infrastructure changes taking effect April 1, 2026. All integrations must migrate to the new Digital Trust Platform and OIDC-based approach before this deadline.

Integration Method

- **Protocol:** OpenID Connect (OIDC) / OAuth 2.0
- **Flow:** Authorization Code Flow with PKCE (Proof Key for Code Exchange)
- **Redirect-based:** Yes, user redirected to BankID login
- **Next.js Compatibility:** Yes, Auth.js/NextAuth supports BankID NO provider
- **Implementation:** Use well-known OIDC libraries

Technical Requirements:

- Set `acr_values` to `urn:bankid:bis` for biometric authentication
- Verify ID token's `acr` claim includes "LOA=3" (Level of Assurance 3)
- Scopes: `openid`, `profile`, `nnin_altsub` (for Norwegian national identity number)
- Generate nonce and code_verifier for security

Reference Implementation: GitHub - BankID OIDC Integration Examples

Requirements to Get Access

Mandatory Prerequisites:

1. Company must be a customer of a Norwegian bank (within BankID network)
2. Person signing the contract must have personal eID (Norwegian BankID, Swedish BankID, or Danish MitID)
3. Completed "Getting Ready for Production" guide (step 5) to obtain production domain
4. Register application in BankID Developer Portal (freely available)

Application Information Required:

- Company information
- General contact person
- Person authorized to sign agreement
- Norwegian bank details
- Technical contacts (credentials delivery, blocking/revoking access)
- Display name for login app
- Production domain URL

Agreement Process:

1. Submit application information

2. Provider sends online agreement for signing
3. Signed agreement forwarded to your bank for processing
4. Bank issues client credentials

Cost

Direct from BankID Norge (Reseller Model):

- One-time establishment fee: NOK 100,000
- Fixed monthly fee: NOK 8,300
- Per-transaction costs: Not clearly specified in direct model

Via Idura/Criipto Aggregator:

- Monthly platform fee: €65–€390 (tier-dependent: Small/Medium/Large)
- Biometric BankID (app): DKK 0.65 per login
- Traditional BankID: DKK 0.89 per login
- Billing: Monthly consumption + subscription

NEEDS VERIFICATION: Direct BankID pricing may have changed. Contact BankID Norge for current 2026 pricing.

Technical Complexity

Difficulty Level: Medium

Pros:

- Standard OIDC implementation
- Extensive documentation available
- Auth.js/NextAuth built-in support
- Code examples available on GitHub

Cons:

- April 1, 2026 migration deadline adds urgency
- Must handle migration to new Digital Trust Platform
- PAdES transition required for document signing (Jan-Mar 2026)
- More complex setup vs simpler OAuth providers

Estimated Integration Time: 2-4 weeks (including testing and certification)

Timeline

Application to Production:

- Bank processing time: Up to 10 business days after signed agreement
- Total estimated timeline: 2-4 weeks (including application, bank processing, credential issuance)

Critical Dates:

- **January 1, 2026:** PAdES transition begins for Enterprise/Express API
- **March 31, 2026:** Final deadline for PAdES migration
- **April 1, 2026:** Old BankID Server and OIDC signing from Stø discontinued

Action Required: Complete migration to Digital Trust Platform before April 1, 2026.

Sandbox/Test Environment

Test Access: Freely available

Test Environment Details:

- Register application in BankID Developer Portal (free)
- Preprod app access: Request via support portal or through BankID partner
- Self-service test user portal: ra-preprod.bankidnorge.no
- Default test credentials: OTP password and qwer1234
- Test users: Generate Norwegian national identity numbers (NNIN) for testing

Testing Tools:

- Available at tools.bankid.no
- Supports authentication, signing, password change
- Document types: plain text, PDF, XML
- Can be embedded via iframe or direct link

Support: developer@bankidnorge.no

PSD2 Relevance

SCA Compliance: YES - Fully compliant

BankID with biometrics is approved for payments and meets Strong Customer Authentication (SCA) requirements according to PSD2 and 3D Secure standards.

Technical Details:

- Level of Assurance: "Substantial" (eIDAS standard)
- Authentication: WebAuthn-based biometrics (built-in phone/computer biometrics)

- Security: BankID never accesses biometric data; receives signed confirmation from Apple/Google
- PSD2 Integration: Netcompany Banking Services supports 1-SCA (single strong customer authentication) using BankID for Norway

Use Cases for Drop:

1. User authentication/login
2. PSD2 payment authorization (SCA)
3. Combined auth + payment flow

Alternative Providers

Aggregator Services (Recommended):

1. **Idura (formerly Criipto)**
   - Bundles BankID + Vipps + other Nordic eIDs
   - Single integration point for multiple providers
   - Pricing: €65-€390/month + per-transaction fees
   - Website: idura.eu
2. **Signicat**
   - Largest BankID provider in Norway (established 2007)
   - Enterprise-focused solution
   - Offers authentication + digital signatures
   - Pricing: Contact for quote
   - Website: signicat.com
3. **Curity**
   - Identity platform with Norwegian BankID support
   - OIDC authenticator approach
   - Enterprise-grade solution
   - Website: curity.io

Recommendation: For Drop's use case (fintech startup), Idura offers the best balance of simplicity, cost-effectiveness, and multi-provider support.

---

2. Vipps Login

What is it?

Vipps is Norway's #1 mobile payment provider with near-ubiquitous adoption. Vipps Login is an authentication service that allows users to log in using their mobile number. The brand split: Vipps

(Norway/Sweden) and MobilePay (Denmark/Finland) use the same API under Vipps MobilePay.

Scope: Login API confirms customer identity and provides access to verified data: name, birthdate, social security number, address, email, phone number.

Integration Method

- **Protocol:** OpenID Connect (OIDC) / OAuth 2.0
- **Flow:** Browser-based redirect flow (user-initiated or merchant-initiated)
- **Authentication:** API keys (obtained via Vipps MobilePay business portal)
- **Next.js Compatibility:** Yes, Auth.js/NextAuth supports Vipps MobilePay provider
- **Age Requirement:** Users must be 15+ years old

Implementation Example:

```
import NextAuth from "next-auth"
import Vipps from "next-auth/providers/vipps"

export const { handlers, auth, signIn, signOut } = NextAuth({
  providers: [Vipps],
})
```

Test Mode Override:

```
Vipps({ issuer: "https://apitest.vipps.no/access-management-1.0/access/" })
```

Key Endpoint:

- User info: GET:/vipps-userinfo-api/userinfo (returns consented user data)
- Token endpoint: Standard OIDC token exchange

Requirements to Get Access

Application Process:

1. Order product at vippsmobilepay.com
2. Complete "Login checklist" for direct integration
3. Partner application review
4. Receive test credentials via email (test phone number + national identity number)

Company Requirements:

- NEEDS VERIFICATION: Minimum company requirements not specified in documentation
- Likely requires Norwegian business registration

Technical Setup:

- Access business portal: portal.vippsmobilepay.com
- Obtain API keys for authentication
- Configure redirect URIs

Cost

Per-Transaction Pricing:

- Login without SSN: DKK 0.00 (FREE)
- Login with SSN: DKK 0.40

Via Idura Aggregator:

- Monthly platform fee: €65–€390 (tier-dependent)
- Per-transaction: Vipps MobilePay invoices directly based on "active users" pricing model
- NEEDS VERIFICATION: Current 2026 active users pricing structure

Notes:

- Most cost-effective authentication option
- Free basic login is suitable for initial authentication
- SSN access (DKK 0.40) needed for age/identity verification

Technical Complexity

Difficulty Level: Low-Medium

Pros:

- Standard OIDC/OAuth2 implementation
- Excellent documentation
- Auth.js built-in support
- Well-known integration libraries recommended
- Active GitHub repositories with examples
- Widespread usage in Norway (proven reliability)

Cons:

- Test environment has no SLA/uptime guarantee
- Support limited to Norwegian office hours for test environment
- Separate test and production API keys required

Estimated Integration Time: 1-2 weeks

Timeline

Application to Production:

- NEEDS VERIFICATION: Specific timeline not documented
- Process: Order product → Partner review → Credentials issued
- Estimated: Likely 1-2 weeks based on industry standards

Recommendation: Contact Vipps developer support for exact onboarding timeline.

Sandbox/Test Environment

Test Environment: Merchant Test (MT) - Available to all API merchants

Access Details:

- All partners/merchants with API access have test environment access
- Test server: https://apitest.vipps.no
- Portal access: portal.vippsmobilepay.com → "For developers" → "Test users"
- Test app: iOS and Android apps that mirror production (connect to MT environment)

Test User Credentials:

- Provided via email after partner review
- Includes test phone number and national identity number
- PIN for "Verify your number": 1236
- PIN for "Enter your code": 1236

Limitations:

- No SLA or uptime guarantee
- No fixes outside Norwegian office hours
- Completely separate from production (different API keys)

Suitable For: Websites, e-commerce, apps, loyalty programs

PSD2 Relevance

SCA Compliance: YES - Fully compliant

Vipps has implemented PSD2-compliant Strong Customer Authentication with regulatory-approved delegated SCA from card issuers.

Technical Details:

- Two-factor authentication: PIN or biometrics + device possession
- No additional 3D Secure required (Verified by Visa, Mastercard ID Check)
- Security handled when user logs into Vipps/MobilePay app
- Wallet-based payment method with built-in SCA layer

Use Cases for Drop:

1. User authentication/login
2. PSD2 payment authorization
3. Simplified payment flow (no separate 3DS step needed)

Advantage: Vipps SCA is transparent to users (already authenticated in app), creating smoother UX than traditional 3DS flows.

Alternative Providers

Same aggregators as BankID:

1. **Idura (formerly Criipto)**
   - Bundles Vipps with BankID and other eIDs
   - Single integration, multiple auth methods
   - Transparent pricing model
2. **Signicat**
   - Enterprise solution
   - Combined authentication suite
   - Contact for pricing

Recommendation: If implementing both BankID AND Vipps, use Idura aggregator to manage both via single integration point.

---

3. Aggregator Comparison

Why Use an Aggregator?

Benefits:

1. Single integration point for multiple eID providers
2. Simplified SDK/API (abstraction layer)
3. Unified billing and reporting
4. Faster time-to-market
5. Reduced maintenance burden
6. Future-proof (easy to add more eID methods)

Trade-offs:

1. Additional monthly platform fee (€65-€390)
2. Dependency on third-party service
3. Potential slight latency increase

Idura (Criipto) - Recommended

What is it: European eID verification platform (formerly Criipto, rebranded to Idura)

Supported eIDs:

- Norwegian BankID (Traditional + Biometric)
- Vipps Login
- Swedish BankID
- Danish MitID
- Finnish eID
- 30+ other European eIDs

Pricing Structure:

- Platform fee: €65/month (Small), €140/month (Medium), €390/month (Large)
- Norwegian BankID: DKK 0.65 (biometric) or DKK 0.89 (traditional) per login
- Vipps: DKK 0.00 (no SSN) or DKK 0.40 (with SSN) per login
- Swedish BankID: DKK 0.10 per login

Technical:

- OIDC/OAuth2 standard
- SDKs available
- Good documentation
- Test environment included

Best For: Drop's use case - need both BankID + Vipps with potential Nordic expansion

Signicat - Enterprise Alternative

What is it: Europe's largest eID and signature provider (established 2007)

Position: Largest BankID provider in Norway

Pricing: Contact for quote (not publicly listed)

Best For: Large enterprises, complex compliance needs, high-volume applications

Direct Integration vs Aggregator

For Drop, Recommend: Idura Aggregator

Reasoning:

1. Supports both BankID and Vipps through one integration
2. Transparent pricing (€140/month Medium tier likely sufficient)
3. Future-proof for Nordic expansion
4. Faster development (proven SDK)
5. Lower maintenance burden
6. Cost-effective at expected volume (<10,000 logins/month)

Break-even Analysis:

- Idura Medium: €140/month + per-transaction fees
- Direct BankID: NOK 8,300/month (€750) + NOK 100,000 setup (€9,000)
- Conclusion: Idura cheaper until very high volumes (50,000+ logins/month)

---

4. Implementation Recommendations

Recommended Approach

Phase 1: Email + Password (MVP)

- Implement JWT-based auth with jose (already planned)
- Collect email, validate age/residency through form
- Manual verification initially

Phase 2: Add BankID (Primary eID)

- Integrate via Idura
- Use BankID for identity verification (name, SSN, address)
- Automatic age verification (18+)
- Satisfies regulatory requirements
- Serves as SCA for PSD2 payments

Phase 3: Add Vipps Login (Alternative)

- Same Idura integration (minimal additional work)
- Offer choice: BankID or Vipps
- Vipps likely preferred by users (more familiar, used daily)
- Free basic login reduces costs

Phase 4: Optimize Flow

- Optional: Allow email/password for returning users
- Require BankID/Vipps for first-time verification
- Re-verify periodically (e.g., annually) via eID

Technical Architecture

Recommended Stack:

```
Next.js 16 App Router
├─ Auth.js (NextAuth v5) - OIDC client
├─ Idura Verify - eID aggregator
│  ├─ Norwegian BankID
│  └─ Vipps Login
├─ jose - JWT signing/verification
└─ PostgreSQL - user sessions
```

Flow:

1. User clicks "Log in with BankID" or "Log in with Vipps"
2. Next.js redirects to Idura OIDC endpoint
3. Idura redirects to BankID/Vipps
4. User authenticates
5. Idura returns to callback with ID token
6. Next.js validates token, extracts claims (name, SSN, email)
7. Create/update user in database
8. Issue JWT session token (jose)
9. User authenticated

Security Considerations:

- Store Idura client credentials in environment variables
- Validate ID token signature
- Check `acr` claim for LOA=3
- Verify age from birthdate/SSN
- Log all authentication events
- Implement rate limiting

Timeline Estimate

Development Timeline:

- Week 1-2: Idura account setup, test environment configuration

- Week 3-4: Next.js Auth.js integration, BankID flow
- Week 5: Vipps Login integration
- Week 6-7: Testing, edge cases, error handling
- Week 8: Production deployment, monitoring

Total: 8 weeks to production-ready dual eID authentication

Cost Projection (First Year)

Assumptions:

- 1,000 users in year 1
- 50% use BankID, 50% use Vipps
- Average 12 logins/user/year
- Idura Medium tier: €140/month

Calculation:

- Platform fee: €140 × 12 = €1,680
- BankID logins: 500 users × 12 logins × DKK 0.65 = DKK 3,900 (€470)
- Vipps logins: 500 users × 12 logins × DKK 0.40 = DKK 2,400 (€290)
- **Total Year 1:** €2,440

At Scale (10,000 users):

- Platform fee: €1,680
- BankID: €4,700
- Vipps: €2,900
- **Total:** €9,280/year

Conclusion: Cost scales linearly with users, remains affordable for fintech startup.

---

5. Risks and Mitigations

BankID Migration Risk (Critical)

Risk: April 1, 2026 deadline for Digital Trust Platform migration

Impact: Service disruption if not migrated in time

Mitigation:

- If integrating via Idura: Migration handled by aggregator
- If direct integration: Prioritize migration work immediately
- Test new platform in preprod before March 31
- **Recommendation:** Use Idura to offload migration risk

Age Verification Accuracy

Risk: Users might bypass age check with email/password

Mitigation:

- Require BankID/Vipps for account activation
- Email/password only for returning users
- Periodic re-verification (annual)
- Flag accounts without eID verification

User Adoption

Risk: Users unfamiliar with eID login may abandon signup

Mitigation:

- Clear onboarding instructions
- Video tutorial for first-time users
- Support contact readily available
- Fallback to manual verification if needed

Service Availability

Risk: BankID/Vipps downtime prevents login

Mitigation:

- Multiple authentication options (BankID + Vipps)
- Cache authentication status (JWT sessions)
- Monitor provider status pages
- Implement graceful degradation

Regulatory Changes

Risk: PSD2/eIDAS requirements may change

Mitigation:

- Use compliant providers (BankID/Vipps are regulated)
- Stay informed via provider newsletters
- Idura handles compliance updates
- Legal review of authentication flow

---

6. Questions Needing Verification

The following points require direct contact with providers for confirmation:

1. **BankID Direct Pricing:** Current 2026 per-transaction costs (NOK 8,300/month model unclear on variable costs)
2. **Vipps Timeline:** Exact onboarding timeline from application to production
3. **Vipps Active Users Model:** Current 2026 pricing structure for active users billing
4. **Idura Large Tier:** Volume thresholds for Small/Medium/Large tiers
5. **Minimum Requirements:** Specific business registration requirements for Vipps merchant account
6. **SCA Dual-Use:** Confirm BankID/Vipps can be used for BOTH login and payment authorization in same session
7. **April 2026 Migration:** Detailed requirements if integrating direct BankID (not via aggregator)

---

7. Final Recommendation

Recommendation: Implement BOTH BankID and Vipps via Idura aggregator

Justification:

1. **Regulatory Compliance:** BankID satisfies identity verification (18+, Norwegian resident)
2. **User Preference:** Vipps more familiar, offers free login option
3. **PSD2 Dual-Use:** Both serve as authentication AND SCA for payments
4. **Cost-Effective:** Idura cheaper than direct integration until high volume
5. **Risk Mitigation:** Idura handles April 2026 BankID migration
6. **Future-Proof:** Easy to add Swedish/Danish eIDs for Nordic expansion
7. **Development Speed:** Faster implementation with proven SDK

Implementation Priority:

1. Phase 1: Email/Password (MVP launch)
2. Phase 2: BankID via Idura (compliance requirement)
3. Phase 3: Vipps via Idura (user convenience)

Next Steps:

1. Contact Idura sales for Medium tier quote and setup
2. Register test account and explore SDK documentation
3. Validate integration with Next.js 16 App Router
4. Architect user database schema (with eID verification fields)
5. Implement BankID flow first (higher priority for compliance)
6. Add Vipps as alternative option
7. Load test authentication flow
8. Production deployment with monitoring

Sources

BankID Sources

- Norwegian BankID Integration Using the OIDC Authenticator | Curity
- Norwegian BankID - STØ Changes | Signicat
- Norwegian BankID Developer Pages | Signicat
- GitHub - BankID API Documentation
- Integration Guide for Norwegian BankID | Signicat
- Auth.js | Bankid No
- BankID Norge Pricing
- Norwegian BankID - Easy Authentication & Signatures | Idura
- BankID Norway Developer Portal
- Testing - BankID Documentation
- OpenID Connect Authorization Code Flow
- GitHub - BankID OIDC Integration Examples
- BankID: Norway's Digital ID System Explained - Life in Norway

Vipps Sources

- Introduction to the Login API | Vipps MobilePay Developer Docs
- Login API | Vipps MobilePay Developer Docs
- Vipps Login Integration - Norwegian Authentication | spektr
- API Platform Overview | Vipps MobilePay Developer Docs

- Vipps Login - Convenient eID Authentication | Idura
- Vipps MobilePay · GitHub
- Login | Vipps MobilePay Pricing
- Auth.js | Vipps MobilePay
- Integrate Login from a Website | Vipps MobilePay Developer Docs
- Vipps MobilePay Test Environment

PSD2/SCA Sources

- PSD2 and Strong Customer Authentication | Criipto
- FAQ Biometrics | BankID
- PSD2 News | Netcompany
- Direct Integration and PSP Integration | Vipps MobilePay
- Strong Customer Authentication | Frisbii Docs

Aggregator Sources

- Pricing Idura Verify
- Pricing - Signicat
- Electronic Identities | Criipto
- Partners - Authentication | BankID
- Criipto (BankID, Vipps) - Seamless Insure

Report Prepared By: John (AI Director) **Last Updated:** 2026-02-15 **Status:** Research complete, awaiting approval for implementation

Cloud Cost Analysis

Drop — Cloud Deployment Cost Analysis

Date: 2026-02-11 **Author:** John (AI Director) **Status:** Historical — superseded by ADR-014 (PostgreSQL-only) and ADR-012 (AWS App Runner)

> **NOTE (2026-03-03):** This analysis was written before ADR-014 mandated PostgreSQL 16 in all environments. SQLite references below reflect the old architecture and are no longer valid. Current deployment: AWS App Runner + AWS RDS PostgreSQL 16. See ADR-012 and ADR-014.

Current Tech Stack

Layer	Tech	Production Note
App	Next.js 16 (App Router)	Monolith, ~7 pages + API
Frontend	React 19 + Tailwind v4	SSR/SSG
DB	SQLite (better-sqlite3)	Must migrate to PostgreSQL for production
Auth	JWT (jose) httpOnly cookie	OK for production
Dependencies	bcryptjs, radix-ui, lucide, sonner	Lightweight
Dev server	Port 3001 (configured in project.json)	Currently running locally

Key constraint: SQLite cannot handle concurrent writes (ADR-001). Must switch to PostgreSQL before launch.

Phase 1: MVP / Demo (now ? 200 users)

Provider	Plan	Price/mo	Notes
Vercel Pro	Next.js native	$20 (~215 NOK)	No persistent FS — SQLite won't work without Turso/Neon
Railway Starter	Next.js + persistent disk	$5 + usage (~160 NOK)	SQLite works here
Fly.io Hobby	LiteFS support	$5 + usage (~160 NOK)	Great for SQLite
Hetzner VPS (shared)	On same CPX41	+~0 NOK	If already provisioned from system migration

Recommended Phase 1 Stack

Item	Provider	Cost/mo
App hosting	Hetzner VPS (shared) or Railway	0-160 NOK
DB	SQLite (local)	0
Domain	getdrop.no (one.com)	~100 NOK/yr
SSL	Let's Encrypt / Cloudflare	0
Total Phase 1		**~10-170 NOK/mo**

Phase 2: Launch (200-3,000 users)

SQLite → PostgreSQL migration required. Need transactional email and SMS for auth.

Item	Provider	Cost/mo
App hosting	Railway or Fly.io	$10-20 (~110-215 NOK)
PostgreSQL managed	Neon free→Pro $19 or Supabase free→$25	0-270 NOK
Transactional email	Resend (3,000 free/mo) → $20	0-215 NOK
SMS (OTP auth)	Twilio ~$0.05/SMS × 500/mo	~270 NOK
CDN	Cloudflare Free	0
Monitoring	Sentry free tier	0
BaaS (Wise API)	Per-transaction fee	Covered by tx fees

Item	Provider	Cost/mo
Total Phase 2		**~400-1,000 NOK/mo**

Phase 3: Scale (3,000-15,000 users)

Fintech = reliability, backups, WAF, logging required.

Item	Provider	Cost/mo
App hosting (2 instances)	Railway Pro or Fly.io	$30-50 (~325-540 NOK)
PostgreSQL managed (HA)	Neon Pro $69 or Supabase Pro $25+usage	270-750 NOK
Redis (caching/sessions)	Upstash free→$10	0-110 NOK
Transactional email	Resend Pro $20	215 NOK
SMS (OTP)	Twilio × 3,000/mo	~1,600 NOK
CDN + WAF	Cloudflare Pro $20	215 NOK
Monitoring	Sentry Team $26	280 NOK
Logging	Betterstack free→$25	0-270 NOK
Backup storage	Backblaze B2	55 NOK
BaaS APIs (Wise/Thunes/Swan)	Per-tx, variable	Covered by tx fees
Total Phase 3		**~3,000-4,000 NOK/mo**

Summary

Phase	Users	Infra cost/mo	MRR (from business case)	Margin
MVP	0-200	10-170 NOK	0-12,000 NOK	— (pre-revenue)
Launch	200-3,000	400-1,000 NOK	12,000-130,000 NOK	90%+
Scale	3,000-15,000	3,000-4,000 NOK	130,000-650,000 NOK	97%+

Infrastructure cost is negligible vs revenue. Fintech margins on infra are excellent — biggest costs are marketing (30-50K/mo) and compliance, not hosting.

Shared Hetzner VPS Option

Drop can run on the same Hetzner CPX41 (from system migration analysis) for +0 NOK incrementally:

- Next.js production build → Docker container
- PostgreSQL → share existing Docker Postgres or add new container
- Cloudflare tunnel: add new hostname for Drop

Only at 3,000+ users should Drop move to dedicated infrastructure.

Related

- System cloud migration analysis: ~/ALAI/finance/cloud-migration-analysis.md (MC #524)
- Drop business case: ~/ALAI/products/Drop/project/docs/zica-business-case-v2.md
- Drop architecture: ~/ALAI/products/Drop/project/architecture/architecture-document.md