drop-srbija-plan

Plan: Drop Srbija — Phase 2 Build Plan

Created: 2026-04-16 **Product:** Drop Srbija — Serbian market phone-based payment app
Scaffold: ~/ALAI/products/DropSrbija/ **Status:** Scaffold complete. Phase 2 build begins.

Research Summary (5-Expert Gap Analysis)

Critical Discoveries

#	Finding	Severity	Expert
1	NBS IPS is ISO 20022 XML via mTLS — NOT REST. Blueprint's `https://ips.nbs.rs/api/v1` endpoint DOES NOT EXIST	P0	Markos Zachariadis
2	Drop cannot connect to NBS IPS directly — must go through a licensed bank partner	P0	Markos Zachariadis
3	No Serbian d.o.o. legal entity → NBS PI license application impossible	P0	Thaer Sabri
4	No NBS PI license application initiated — operating live IPS is criminal violation	P0	Thaer Sabri
5	OTP stored as `hash($otp)` = plaintext string — NOT bcrypt. Security theater.	P0	Petter Graff / Angie Jones

#	Finding	Severity	Expert
6	Phone-to-IBAN resolution missing — NBS IPS needs IBAN, not phone. No Serbian registry exists	P0	Markos Zachariadis
7	Phase 3 (live IPS) BEFORE Phase 4 (KYC) = ZPNFTM AML violation — sequence is illegal	P0	Thaer Sabri
8	69 test cases needed, 0 exist. No test infrastructure, no src/test directory	P0	Angie Jones
9	NBS IPS P2P transfers are FREE by regulation — per-transaction fee model impossible for consumers	P1	Markos Zachariadis + BA
10	IPS QR must use DinaCard standard — custom HMAC QR unreadable by all Serbian bank apps	P1	Markos Zachariadis
11	No SMS provider integrated (Twilio referenced but not implemented)	P1	Petter Graff
12	Sanctions screening references "NBS SDN list" — doesn't exist. Must use UN + EU + Serbian lists	P1	Thaer Sabri
13	Pre-transaction disclosure screen missing — legally required by Law on Payment Services	P1	Thaer Sabri
14	USPNFT AML reporting module entirely absent from architecture	P1	Thaer Sabri
15	No CI/CD pipeline, no Dockerfile, no docker-compose.yml for DropSrbija	P1	Petter Graff

Revenue Model Reality

- **Consumer P2P:** Must be FREE (NBS regulation mandate)
- **Merchant QR:** 0.5–1.2% per transaction (competitive vs. card at 1.5–1.8%)
- **B2B payroll:** Flat fee per batch
- **NBS IPS cap:** 300,000 RSD (~€2,550) per transaction hard limit
- **Bank partner timeline:** 12–18 months to live IPS integration

CEO-Level Decisions Required

1. **Incorporate Drop Srbija d.o.o. in Serbia** — min capital EUR 125,000
2. **Bank partner outreach** — Priority: Raiffeisen Serbia, MTS Banka (Telekom Srbija subsidiary — phone data synergy)
3. **NBS PI license application** — 12–14 months, requires Serbian legal counsel

---

Objective

Build Drop Srbija from scaffold to production-ready MVP: fix all P0 security/legal blockers, implement bank partner adapter architecture, build KYC/AML compliance layer, write 69+ test cases, set up CI/CD — in correct regulatory sequence (KYC → IPS, not IPS → KYC).

Team Orchestration

Team Members

ID	Name	Role	Company	Agent Type
B1	petter-graff	Backend architecture + security fixes	CodeCraft	backend-builder
B2	finverge	Payments compliance + AML architecture	Finverge	finverge
B3	lexicon	Legal docs + ZZPL compliance	Lexicon	lexicon
B4	proveo	QA — all test suites	Proveo	proveo
B5	flowforge	DevOps — CI/CD, Docker	FlowForge	devops-dev
B6	vizu	Frontend — disclosure screens, complaints UI	Vizu	vizu
V1	angie-jones	Test validation — all builds	Proveo	angie-jones
V2	sentinel-validator	Cross-reference final report	SENTINEL	sentinel-validator

---

Step-by-Step Tasks

Phase 0: CEO Decisions (Escalated — Not Delegated to Builders)

Task 0a: Incorporate Drop Srbija d.o.o. + initiate NBS PI license

- Owner: Alem Basic (CEO)
- Estimated cost: EUR 125,000 minimum capital + Serbian legal counsel fees
- Lexicon can draft the application package; Serbian advocate must sign/submit
- Timeline: 12–18 months to authorization

Task 0b: Bank partner outreach

- Priority 1: Raiffeisen Bank Srbija (developer portal, fintech-friendly)
- Priority 2: MTS Banka (Telekom Srbija — phone-to-IBAN synergy)
- Documents prepared by: sentinel-ba (Task 10 below)

Phase 1: Security P0 Fixes (CodeCraft)

Task 1: Fix OTP Security (CRITICAL BLOCKER)

- Owner: B1 (petter-graff)
- BlockedBy: none
- Acceptance:
  - ☐ `PhoneOtpService.hashOtp()` uses bcrypt (BCrypt.hashpw, cost factor 12)
  - ☐ `PhoneOtpService.verifyOtpHash()` uses BCrypt.checkpw
  - ☐ Stored OTP in DB is bcrypt hash, not `"hash($otp)"` string
  - ☐ Existing unit tests pass (or are updated to match)
  - ☐ No plaintext OTP ever written to logs

Task 2: Fix Phone Regex + Add Serbian Format Normalisation

- Owner: B1 (petter-graff)
- BlockedBy: none
- Acceptance:
  - ☐ Regex updated: `^\+381[0-9]{8,9}$` (8–9 digits after country code)
  - ☐ Normalisation: `0641234567` → `+381641234567` at route layer
  - ☐ Landline prefix (+38111, +38121 etc.) rejected for OTP

- [ ] Test fixtures documented in code

Task 3: Per-Phone OTP Rate Limiting

- Owner: B1 (petter-graff)
- BlockedBy: none
- Acceptance:
  - [ ] 3 OTP requests per phone per minute → 4th returns 429
  - [ ] 10 OTP requests per phone per hour → returns 429
  - [ ] Redis used as rate limit store (already in docker-compose)
  - [ ] Rate limit headers in response (X-RateLimit-Remaining)

Task 4: SMS Provider Integration (SmsGateway abstraction + Twilio)

- Owner: B1 (petter-graff)
- BlockedBy: Task 1
- Acceptance:
  - [ ] `SmsGateway` interface with `sendOtp(phone: String, otp: String): SmsResult`
  - [ ] `TwilioSmsGateway` implementation using Twilio REST API
  - [ ] `StubSmsGateway` for dev/test (prints OTP to logs)
  - [ ] `PhoneOtpService` injects `SmsGateway` (DI via Koin/manual)
  - [ ] Twilio credentials from environment variables (not hardcoded)
  - [ ] ENV: TWILIO_ACCOUNT_SID, TWILIO_AUTH_TOKEN, TWILIO_FROM_NUMBER

Task 5: Validate Task 1–4 (Security Fixes)

- Owner: V1 (angie-jones)
- BlockedBy: Tasks 1, 2, 3, 4
- Acceptance:
  - [ ] OTP in `phone_verifications` table is bcrypt hash (verified via SELECT)
  - [ ] Attempting brute force OTP (6 wrong guesses) returns correct HTTP 400
  - [ ] 4th OTP request in 1 minute returns HTTP 429
  - [ ] Phone `+381123456` (too short) rejected at route layer

Phase 2: Architecture (CodeCraft)

Task 6: NBS IPS Bank Partner Adapter Pattern

- Owner: B1 (petter-graff)
- BlockedBy: Task 1

- Acceptance:
  - ☐ `BankPartnerAdapter` interface with `initiateTransfer()`, `checkStatus()`, `resolvePhoneToAccount()`
  - ☐ `StubBankPartnerAdapter` — realistic mock with ISO 20022 status codes (ACCP, ACSC, RJCT, PDNG)
  - ☐ `RaiffeisenBankAdapter` — skeleton with mTLS config hooks
  - ☐ Amount validation: `amount > 300_000 RSD` → HTTP 422 `AMOUNT_EXCEEDS_IPS_LIMIT`
  - ☐ `NbsIpsLogs.request_body` stores ISO 20022 XML (not JSON stub)
  - ☐ `partner_bank` column added via Flyway V2 migration

Task 7: Phone-to-IBAN Resolution Layer

- Owner: B1 (petter-graff)
- BlockedBy: Task 6
- Acceptance:
  - ☐ `linked_accounts` table via Flyway V3 (id, user_id, iban, bank_name, is_primary, verified_at)
  - ☐ IBAN validation: Serbian RS + 20 digits with checksum
  - ☐ `AccountLinkingService.resolvePhoneToIban(phone)` returns primary IBAN or null
  - ☐ `GET /v1/accounts`, `POST /v1/accounts/link`, `PATCH /v1/accounts/{id}/set-primary`
  - ☐ `POST /v1/ips/initiate` returns 404 `RECIPIENT_NOT_REGISTERED` if phone not linked
  - ☐ Onboarding flow requires IBAN link before first payment

Task 8: Transaction Idempotency

- Owner: B1 (petter-graff)
- BlockedBy: Task 7
- Acceptance:
  - ☐ `Idempotency-Key` header on `POST /v1/ips/initiate`
  - ☐ Duplicate request with same key returns original response (not double charge)
  - ☐ Idempotency key stored in Transactions table
  - ☐ 60-minute idempotency window

Task 9: Validate Task 6–8 (Architecture)

- Owner: V1 (angie-jones)
- BlockedBy: Tasks 6, 7, 8
- Acceptance:
  - ☐ POST /v1/ips/initiate with amount 300,001 → HTTP 422
  - ☐ POST /v1/ips/initiate to unlinked phone → HTTP 404

- [ ] Duplicate initiate with same Idempotency-Key → single transaction in DB

Phase 3: Compliance Architecture (Finverge + CodeCraft)

Task 10: KYC Service (Veriff/Sumsub + JMBG)

- Owner: B2 (finverge)
- BlockedBy: Task 6
- Acceptance:
  - [ ] `KycService.kt` with `createKycSession()`, `handleKycWebhook()`, `updateKycStatus()`
  - [ ] `kyc_sessions` table via Flyway V5
  - [ ] JMBG field added to Users: `jmbg_encrypted`, `jmbg_hash` (Flyway V6)
  - [ ] `KycRequiredPlugin` gates `/v1/ips/initiate` → 403 if kyc_status ≠ VERIFIED
  - [ ] Human-in-the-loop review step before VERIFIED status
  - [ ] Phase sequence enforced: KYC BEFORE live IPS

Task 11: AML Monitoring + USPNFT Reporting

- Owner: B2 (finverge)
- BlockedBy: Task 10
- Acceptance:
  - [ ] Velocity rules: flag user exceeding 120,000 RSD in 24h
  - [ ] Structuring detection: multiple sub-threshold transactions in pattern
  - [ ] STR workflow: alert → compliance review → USPNFT eUprava export (XML)
  - [ ] Sanctions screening: UN consolidated + EU restrictive + Serbian Government lists
  - [ ] All references to "NBS SDN list" removed/corrected in codebase + docs
  - [ ] `aml_flags` table with risk_level, flag_reason, reviewed_by, resolved_at

Task 12: Pre-Transaction Disclosure + Post-Settlement Receipt

- Owner: B1 (petter-graff) backend + B6 (vizu) frontend
- BlockedBy: Task 11
- Acceptance:
  - [ ] Confirmation screen before POST /v1/ips/initiate: amount, fee, execution time, exchange rate
  - [ ] `disclosure_acknowledged: true` flag in initiation payload + stored in Transactions
  - [ ] NBS IPS settlement webhook handler → push notification/in-app receipt

- [ ] Receipt contains: tx reference, amount, fee, value date, recipient ID
- [ ] Flyway migration adds `disclosure_acknowledged` to Transactions table

Task 13: Complaints Handling Module

- Owner: B1 (petter-graff) backend + B6 (vizu) frontend
- BlockedBy: Task 12
- Acceptance:
  - [ ] `complaints` table (id, user_id, transaction_id, category, status, submitted_at, resolved_at)
  - [ ] `POST /v1/complaints` (authenticated user)
  - [ ] `GET /admin/complaints` (compliance officer)
  - [ ] SLA alert: flag if complaint > 10 working days unresolved
  - [ ] Resolution letter template in Serbian with NBS escalation notice

Task 14: Legal Documents Package (Lexicon)

- Owner: B3 (lexicon)
- BlockedBy: none (parallel)
- Acceptance:
  - [ ] Privacy policy in Serbian (ZZPL Article 23 compliant)
  - [ ] DPIA for KYC biometric processing (ZZPL Article 54)
  - [ ] NBS PI license application package (business plan, org chart, AML programme)
  - [ ] Framework contract for payment service users (Serbian, Law on Payment Services Articles 60-70)
  - [ ] NBS PISP license requirements checklist
  - [ ] Bank partnership pitch document
  - [ ] Incident notification procedure (NBS 4h initial, NBS 72h detailed, Poverenik 72h)
  - [ ] All saved to: ~/ALAI/products/DropSrbija/comms/decisions/

Task 15: Validate Task 10–13 (Compliance)

- Owner: V1 (angie-jones)
- BlockedBy: Tasks 10, 11, 12, 13
- Acceptance:
  - [ ] User with kyc_status = PENDING cannot initiate payment → 403
  - [ ] Payment attempt with sanctioned phone → 403 + audit log entry
  - [ ] Complaint submission → DB record + SLA timer started
  - [ ] Disclosure screen appears before payment confirmation

---

Phase 4: DevOps (FlowForge)

Task 16: Dockerfile + Docker Compose for DropSrbija

- Owner: B5 (flowforge)
- BlockedBy: Task 4 (SMS env vars needed)
- Acceptance:
  - ☐ `Dockerfile.drop-srbija-api` with non-root user (uid 1001)
  - ☐ Multi-stage build (builder + runtime)
  - ☐ `docker-compose.yml` with all 4 services: postgres:5434, redis:6380, api:3003, frontend:3000
  - ☐ `docker-compose.production.yml` with SEED_DEMO=false
  - ☐ Health checks on all containers
  - ☐ `.env.example` with all required variables documented

Task 17: CI/CD Pipeline

- Owner: B5 (flowforge)
- BlockedBy: Task 16
- Acceptance:
  - ☐ `.github/workflows/test.yml` — run Kotest on every PR
  - ☐ `.github/workflows/build.yml` — docker build on push to develop
  - ☐ `.github/workflows/deploy-staging.yml` — deploy to staging on merge to develop
  - ☐ Quality gate: fails if test coverage < 60%
  - ☐ Sonar integration (reuse pattern from Drop Norway)

Task 18: Validate Task 16–17 (DevOps)

- Owner: B5 (flowforge) + V1 (angie-jones)
- BlockedBy: Tasks 16, 17
- Acceptance:
  - ☐ `docker-compose up` starts all 4 containers healthy
  - ☐ `GET http://localhost:3003/health` returns 200
  - ☐ CI pipeline runs on test PR without errors

Phase 5: Test Suites (Proveo + CodeCraft)

Task 19: Kotest + Testcontainers + WireMock Infrastructure

- Owner: B1 (petter-graff)

- BlockedBy: Task 16
- Acceptance:
  - ☐ `build.gradle.kts` test dependencies: kotest-runner-junit5, kotest-assertions-core, testcontainers-postgresql, wiremock-jre8, ktor-server-test-host
  - ☐ `AbstractIntegrationTest` base class: starts PG16 container, runs Flyway, truncates tables between tests
  - ☐ `FakeSmsGateway` implementation
  - ☐ `docker-compose.test.yml` (PG only)
  - ☐ `Makefile` target `make test`

Task 20: PhoneOtpService Tests (10 cases)

- Owner: B4 (proveo)
- BlockedBy: Task 19
- Acceptance:
  - ☐ `PhoneOtpServiceTest.kt` — 10 test cases per Angie Jones spec
  - ☐ OTP bcrypt storage verified
  - ☐ Expiry, attempts lock, re-request all tested
  - ☐ All 10 pass

Task 21: OTP Rate Limiting Tests (5 cases)

- Owner: B4 (proveo)
- BlockedBy: Tasks 3, 19
- Acceptance:
  - ☐ 5 rate limiting scenarios tested
  - ☐ Per-phone independence verified
  - ☐ All 5 pass

Task 22: NBS IPS WireMock Tests (9 cases)

- Owner: B4 (proveo)
- BlockedBy: Tasks 6, 19
- Acceptance:
  - ☐ WireMock stubs for ACCP, RJCT, 500, timeout, 429 scenarios
  - ☐ NbsIpsLogs verified after each scenario
  - ☐ All 9 pass

Task 23: Amount Validation + AML Threshold Tests (19 cases)

- Owner: B4 (proveo)
- BlockedBy: Tasks 8, 11, 19

- Acceptance:
  - [ ] Amount edge cases: 0, -1, MAX_INT, decimal, >300k RSD
  - [ ] AML threshold: >120k RSD flags correctly
  - [ ] Sanctioned phone → 403
  - [ ] All 19 pass

Task 24: JWT Security Tests (10 cases)

- Owner: B4 (proveo)
- BlockedBy: Task 19
- Acceptance:
  - [ ] Wrong issuer, expired, tampered, wrong audience all → 401
  - [ ] 401 responses don't leak internal info
  - [ ] All 10 pass

Task 25: Playwright E2E Tests (6 journeys, Serbian locale)

- Owner: B4 (proveo)
- BlockedBy: Task 16 (needs running stack)
- Acceptance:
  - [ ] `playwright.config.ts` with sr-RS locale, Belgrade timezone, iPhone 14 viewport
  - [ ] 6 user journeys: happy login, invalid phone, wrong OTP, network error, session persist, logout
  - [ ] All 6 pass against running docker-compose stack

Task 26: Validate All Test Suites

- Owner: V1 (angie-jones)
- BlockedBy: Tasks 20, 21, 22, 23, 24, 25
- Acceptance:
  - [ ] `./gradlew test` — all test suites pass
  - [ ] `npx playwright test` — all E2E journeys pass
  - [ ] Total test count ≥ 69
  - [ ] No test suite has 0 tests
  - [ ] Coverage report shows ≥ 60% on modules with tests

Phase 6: Business Development (Skybound/BA)

Task 27: Bank Partnership Outreach Package

- Owner: B2 (finverge) + Skybound BA
- BlockedBy: none (parallel)
- Acceptance:
  - ☐ `serbian-banks-api-landscape.md` — Raiffeisen, MTS Banka, ProCredit, NLB with API capabilities
  - ☐ `serbian-bank-partnership-pitch.md` — one-page pitch deck content
  - ☐ `nbs-pisp-license-requirements.md` — full checklist, capital requirements, timeline
  - ☐ Recommendation: start as bank agent → own license Year 2
  - ☐ Saved to ~/ALAI/products/DropSrbija/comms/decisions/

Phase 7: Validation (End-to-End)

Task 28: Full E2E Scaffold + Feature Validation

- Owner: V1 (angie-jones) + V2 (sentinel-validator)
- BlockedBy: All Phase 1–6 tasks
- Acceptance:
  - ☐ docker-compose up — all 4 containers healthy
  - ☐ OTP flow end-to-end (request → verify → JWT)
  - ☐ IBAN link → IPS initiate → stub PENDING response
  - ☐ KYC gate enforced (unverified user blocked)
  - ☐ AML flag triggered on large transaction
  - ☐ All DB tables exist (8 tables including new ones)
  - ☐ Frontend compiles (`next build`)
  - ☐ Evidence: screenshots, curl outputs, DB query results

Phase 8: Documentation (Skillforge)

Task 29: BookStack Documentation

- Owner: Skillforge
- BlockedBy: Task 28
- Acceptance:
  - ☐ BookStack page: Drop Srbija architecture overview
  - ☐ Regulatory compliance notes (NBS, ZPNFTM, ZZPL)
  - ☐ Developer onboarding guide
  - ☐ Runbook: what to do when NBS IPS goes down

- [ ] Decision log: bank adapter pattern rationale

Validation Commands

```
# Backend tests
cd ~/ALAI/products/DropSrbija/backend
./gradlew test --info

# E2E
cd ~/ALAI/products/DropSrbija/frontend
npx playwright test --reporter=html

# Docker stack
cd ~/ALAI/products/DropSrbija
docker-compose up -d
curl http://localhost:3003/health

# DB check
docker exec -it dropsrbija-postgres psql -U dropsrbija -d dropsrbija_dev -c '\dt'
```

Priority Matrix

Priority	Tasks	Rationale
P0 — Build Now	1, 2, 3, 4, 6, 7, 14, 16, 19	Security, architecture, legal, DevOps foundations
P1 — Build Next	5, 8, 10, 11, 17, 20–25, 27	Compliance, CI, test suites
P2 — Build After	12, 13, 15, 18, 26, 28, 29	UX, validation, docs
CEO Decision	0a, 0b	Capital commitment, bank outreach

Last Updated: 2026-04-16 **Experts consulted:** Markos Zachariadis (Finverge), Thaer Sabri (Lexicon), Angie Jones (Proveo), Petter Graff (CodeCraft), Sentinel BA (Skybound)

Revision #3
Created 2026-04-16 21:46:48 UTC by John
Updated 2026-05-25 07:25:03 UTC by John