Acceptance Criteria: Drop — Fintech Payment App

Acceptance Criteria: Drop — Fintech Payment App

> **Project:** Drop — Remittance + QR Payments **Version:** 1.0 **Date:** 2026-02-23
> **Author:** John (AI Director) **Status:** Approved **Reviewers:** Alem Bašić (CEO)

Document History

Version	Date	Author	Changes
0.1	2026-02-23	John	Initial AC based on integration tests and E2E test suite

---

1. Purpose & Methodology

1.1 What Are Acceptance Criteria?

Acceptance criteria define the conditions under which Drop features are considered done and accepted by the business. They answer: **"How will we know when this feature is done?"**

1.2 Format: Given / When / Then

```
Given [initial context / precondition]
When  [action or event occurs]
```

```
Then  [expected outcome observed]
And   [additional chained outcomes]
```

1.3 Categories

Category	Description
Positive (Happy Path)	System works with valid inputs
Negative (Sad Path)	System handles invalid inputs gracefully
Edge Case	Boundary conditions
Security	Injection, auth, abuse prevention
Compliance	Regulatory requirements

---

2. Feature Acceptance Criteria

Module: Authentication & Onboarding

Feature: User Registration — 3-step Onboarding (FR-001)

Feature Description: New residents register via email + DOB validation → OTP → PIN. BankID replaces DOB in Phase 2. **Business Requirement:** BR-001, BR-002 **Linked User Stories:** US-001

Positive Scenarios:

#	Scenario	Given	When	Then
AC-001	Successful registration	Valid email, password ≥8 chars, Norwegian phone (+47), DOB ≥18 years	User submits registration form	201 created; user proceeds to OTP step; no password hash in response
AC-002	OTP verification passes	Account created; OTP sent to phone	User enters correct 6-digit OTP	User proceeds to PIN setup
AC-003	PIN setup completes	OTP verified	User enters and confirms 4-digit PIN	Account activated; JWT cookie set; redirect to dashboard

Negative Scenarios:

#	Scenario	Given	When	Then

AC-004	Under-18 rejected	DOB indicating age < 18	User submits registration	422 with message "Du må være minst 18 år"
AC-005	Duplicate email	Existing account for email	User submits same email	409 "Email already in use"
AC-006	Missing required field	Registration form	User submits without first_name	422 validation error with field details array
AC-007	Short password	Password < 8 characters	User submits	422 "Password must be at least 8 characters"
AC-008	Invalid phone format	Non-+47 phone number	User submits	422 validation error

Edge Cases:

#	Scenario	Given	When	Then
AC-009	Boundary age (exactly 18)	DOB = today minus 18 years exactly	Registration submitted	Account created successfully
AC-010	Invalid JSON body	Malformed JSON in request	POST /api/auth/register	400 "Invalid JSON body"

Security Acceptance Criteria:

#	Category	Criterion
AC-011	Auth	Password hash not returned in any API response
AC-012	Auth	bcrypt used (hash starts with $2); SHA-256 rejected
AC-013	Rate limiting	10+ registrations from same IP in 1 min → 429

Feature: User Login (FR-002)

Business Requirement: BR-001 **Linked User Stories:** US-002

Positive Scenarios:

#	Scenario	Given	When	Then
AC-020	Successful login	Registered user with valid credentials	POST /api/auth/login	200; JWT in httpOnly cookie; user object returned
AC-021	Authenticated route access	Valid JWT cookie	GET /api/auth/me	200; current user object returned

Negative Scenarios:

#	Scenario	Given	When	Then
AC-022	Wrong password	Registered user	Submits incorrect password	401 "Invalid email or password" (no enumeration)
AC-023	Non-existent email	No account with that email	Login submitted	401 "Invalid email or password" (same error — no enumeration)
AC-024	Rate limiting	10+ login attempts from same IP in 1 minute	Next attempt	429 rate limit response
AC-025	Missing credentials	Empty email or password	Login submitted	400 "Email and password required"

Edge Cases:

#	Scenario	Given	When	Then
AC-026	Invalid JSON	Malformed body	POST /api/auth/login	400 "Invalid JSON body"

Module: Remittance (Send Money)

Feature: Remittance Transaction (FR-020)

Business Requirement: BR-003, BR-005 **Linked User Stories:** US-010

Positive Scenarios:

#	Scenario	Given	When	Then
AC-030	Successful remittance	Authenticated + KYC-approved user; valid recipient; sufficient balance	POST /api/transactions/remittance with amount=1000, currency=RSD	201; transaction created; fee = 5 NOK (0.5%); transaction in history
AC-031	Fee calculation correct	Amount = 2000 NOK	Remittance submitted	fee = 10 NOK; recipient_amount = 2000 NOK (gross)
AC-032	Transaction in history	Successful remittance	GET /api/transactions	Transaction appears with status=completed

Negative Scenarios:

#	Scenario	Given	When	Then
AC-033	Unauthenticated user	No JWT cookie	POST /api/transactions/remittance	401 Unauthorized
AC-034	KYC not approved	kyc_status=pending	Remittance submitted	403 "KYC verification required"
AC-035	Recipient not found	Invalid recipientId	Remittance submitted	404 "Recipient not found"
AC-036	Insufficient balance	Balance < (amount + fee)	Remittance submitted	402 "Insufficient balance"
AC-037	Amount below minimum	amount = 99 NOK	Submitted	400 "Amount must be between 100 and 50000 NOK"
AC-038	Amount above maximum	amount = 50001 NOK	Submitted	400 validation error
AC-039	Invalid amount (NaN)	amount = "abc"	Submitted	400 "Invalid amount"

Compliance Criteria:

#	Category	Criterion
AC-040	AML	Transaction > 50,000 NOK rejected; daily limits enforced
AC-041	Pass-through	No `balance` column in users table; DB test verifies absence

---

Feature: Exchange Rates API (FR-021)

Positive Scenarios:

#	Scenario	Given	When	Then
AC-050	All rates returned	GET /api/rates	Called	6 NOK exchange rates returned (RSD, BAM, PKR, TRY, PLN, EUR)
AC-051	Single rate returned	GET /api/rates/RSD	Called	NOK→RSD rate returned
AC-052	Case insensitive	GET /api/rates/rsd (lowercase)	Called	Same result as /api/rates/RSD

Negative Scenarios:

#	Scenario	Given	When	Then
AC-053	Unsupported currency	GET /api/rates/XXX	Called	404 Not Found

Module: QR Payments

Feature: QR Payment — Consumer (FR-030)

Business Requirement: BR-004, BR-005 **Linked User Stories:** US-020

Positive Scenarios:

#	Scenario	Given	When	Then
AC-060	Successful QR payment	Authenticated + KYC-approved user; valid merchantId; sufficient balance	POST /api/transactions/qr-payment with amount=129, merchantId=valid	201; merchant_fee = 1.29 NOK (1%); transaction created
AC-061	Fee calculation	amount = 200 NOK	QR payment submitted	merchant_fee = 2 NOK (1%)

Negative Scenarios:

#	Scenario	Given	When	Then
AC-062	Invalid merchant	Non-existent merchantId	Payment submitted	404 "Merchant not found"
AC-063	Amount < 1 NOK	amount = 0	Submitted	400 validation error
AC-064	Missing merchantId	No merchantId in body	Submitted	400 "Merchant ID is required"
AC-065	Unauthenticated	No JWT	Submitted	401 Unauthorized

Feature: Merchant Registration + QR Generation (FR-031)

Positive Scenarios:

#	Scenario	Given	When	Then
AC-070	Merchant registered	Authenticated user	POST /api/merchants with business_name, bank_account	Merchant created with unique QR code value
AC-071	QR code retrievable	Registered merchant	GET /api/merchants/me	Merchant details + QR code returned

Module: Security (Cross-cutting)

Feature: Input Validation (FR-001 through FR-080, all)

#	Scenario	Given	When	Then
AC-080	XSS in name field	`<script>alert(1)</script>` as firstName	Registration submitted	422 validation error; no script executed
AC-081	SQL injection in email	`'; DROP TABLE users;--` as email	Registration submitted	422 validation error; no DB mutation
AC-082	10KB password	10,000 character password	Registration submitted	422 "Password too long" or validation error
AC-083	Unicode in name	Bosnian chars (š, đ, ć, č, ž) in name	Registration submitted	201 created; name stored correctly
AC-084	Underage DOB	DOB indicating 17 years old	Registration submitted	422 age validation error

Module: Compliance

Feature: PCI-DSS Card Data Protection (FR-080, Cards feature)

#	Scenario	Given	When	Then
AC-090	No CVV in DB	Cards table	DB schema check	cards table has NO `card_number` or `cvv` columns
AC-091	No balance in users	Users table	DB schema check	users table has NO `balance` column (pass-through model)
AC-092	Only last_four returned	Authenticated user	GET /api/cards/[id]	Response contains `last_four` only; no full card number

3. Integration Scenarios

#	Integration	Scenario	Expected Behavior	Test Environment

INT-001	Sumsub KYC	KYC webhook callback (approved)	User kyc_status updated to 'approved'	Mock webhook in integration tests
INT-002	BaaS PISP	Payment initiation	Transaction recorded; confirmation returned	Mock PISP in NEXT_PUBLIC_SERVICE_MODE=mock
INT-003	BaaS AISP	Balance read from bank	User account balance returned from BaaS	Mock AISP service
INT-004	Exchange rates	Rate data missing	Error handled gracefully; GET /api/rates/XXX → 404	Integration test
INT-005	BaaS unavailable	BaaS API down	System shows user-friendly error; transaction not created	Mocked timeout in tests

---

4. Non-Functional Acceptance Criteria

4.1 Performance

#	Criterion	Target	Test Method
NF-AC-001	bcrypt hashing time	< 1,000ms	api-benchmarks.test.ts
NF-AC-002	Rate limit check time	< 50ms	api-benchmarks.test.ts
NF-AC-003	DB SELECT query	< 10ms	api-benchmarks.test.ts
NF-AC-004	DB INSERT query	< 20ms	api-benchmarks.test.ts
NF-AC-005	50 concurrent rate limit calls	< 2,000ms total	api-benchmarks.test.ts

4.2 Security

#	Criterion	Target	Test Method
NF-AC-010	SHA-256 passwords rejected	verifyPassword returns false for SHA-256 hashes	auth.test.ts
NF-AC-011	JWT tampered tokens rejected	Invalid signature → exception	auth.test.ts
NF-AC-012	Rate limiting blocks after limit	11th request from same IP → 429	middleware.test.ts

#	Criterion	Target	Test Method
NF-AC-013	Input validation completeness	10+ validation test cases pass	validation.test.ts
NF-AC-014	Foreign key constraints enabled	Sessions cannot be created for non-existent users	db.test.ts

4.3 Compliance

#	Criterion	Target	Test Method
NF-AC-020	No balance column in users table	users table schema has no 'balance'	db.test.ts
NF-AC-021	No card_number/cvv in cards table	cards table has no 'card_number' or 'cvv'	db.test.ts
NF-AC-022	Transaction types limited	Only 'remittance' and 'qr_payment' accepted	db.test.ts

---

5. UAT Scenario Mapping

AC ID	AC Description	UAT Scenario ID	Priority
AC-001	Successful registration	UAT-001	Critical
AC-004	Under-18 rejected	UAT-002	Critical
AC-020	Successful login	UAT-003	Critical
AC-030	Successful remittance	UAT-010	Critical
AC-060	Successful QR payment	UAT-020	Critical
AC-090	No CVV in DB	UAT-SEC-001	Critical

---

6. Traceability to Requirements

AC ID	Acceptance Criterion	FR Reference	BR Reference	US Reference
AC-001	Successful registration	FR-001	BR-001	US-001
AC-004	Under-18 rejected	FR-001	BR-002	US-001
AC-020	Successful login	FR-002	BR-001	US-002

AC ID	Acceptance Criterion	FR Reference	BR Reference	US Reference
AC-030	Successful remittance	FR-020	BR-003, BR-005	US-010
AC-060	Successful QR payment	FR-030	BR-004, BR-005	US-020
AC-090	No CVV in DB	FR-080	BR-005, RUL-010	—
NF-AC-020	No balance column	FR-001	BR-005, RUL-003	US-001

> Full traceability matrix: `[requirements-traceability-matrix.md](requirements-traceability-matrix.md)`

Approval

Role	Name	Date	Signature
Author	John (AI Director)	2026-02-23	Approved (AI)
QA Engineer	Validator agent	2026-02-23	Approved (AI)
Product Owner	John	2026-02-23	Approved
AI Director (John)	John	2026-02-23	Approved
CEO (Alem)	Alem Bašić	TBD	

Revision #5
Created 2026-02-23 12:04:51 UTC by John
Updated 2026-05-31 20:03:06 UTC by John