System Context

System Context Diagram (C4 Level 1)

Document: HLD-001 **Status:** Approved **Last updated:** 2026-02-21 **Author:** Standards Architect
Applies to: Drop v1.0 (PSD2 pass-through model)

Overview

This document describes the C4 Level 1 system context for Drop, showing Drop as the central system and all external actors, systems, and regulatory bodies it interacts with. Drop operates as a PSD2 pass-through payment application -- it **never holds customer funds**. User money remains in their bank account at all times.

System Context Diagram

```
graph TB
    subgraph actors["External Actors"]
        sender["Sender<br/>(Norwegian Resident, 18+)<br/>Sends money abroad via PISP"]
        receiver["Receiver<br/>(30+ countries)<br/>Receives remittance"]
        merchant["Merchant<br/>(Norwegian Business)<br/>Accepts QR payments"]
    end

    subgraph drop_system["Drop Payment System"]
        drop["Drop<br/>Next.js 15 + Hono v4<br/>PSD2 Pass-through App<br/>(AISP + PISP)"]
    end

    subgraph banking["Banking & Open Banking"]
        bankid["BankID Norway<br/>OIDC Identity Provider<br/>Strong Customer Authentication"]
        nordic_banks["Nordic Banks<br/>(DNB, SpareBank1, Nordea)<br/>Open Banking
```

```
APIs<br/>AISP: Read balance<br/>PISP: Initiate payment"]
        payment_rails["Payment Rails<br/>SEPA (EEA)<br/>SWIFT (non-EEA)<br/>Remittance
corridors"]
    end

    subgraph compliance["Compliance & KYC"]
        sumsub["Sumsub<br/>KYC/AML Provider<br/>Document verification<br/>PEP/sanctions
screening"]
        finanstilsynet["Finanstilsynet<br/>Norwegian FSA<br/>PISP/AISP
registration<br/>Regulatory oversight"]
        okokrim["Okokrim / EFE<br/>Financial Intelligence Unit<br/>STR/SAR filing"]
    end

    subgraph infrastructure["Infrastructure"]
        aws["AWS App Runner<br/>Container hosting<br/>Auto-scaling"]
        cloudflare["Cloudflare<br/>CDN, DDoS protection<br/>DNS, TLS termination"]
        sentry["Sentry<br/>Error tracking<br/>Performance monitoring"]
    end

    %% Actor interactions
    sender -->|"BankID login\nView balance (AISP)\nSend money (PISP)\nQR payments"| drop
    receiver -.->|"Receives funds\n(via bank transfer)"| payment_rails
    merchant -->|"Register business\nView dashboard\nGenerate QR code"| drop

    %% Banking integrations
    drop -->|"OIDC authorize\nID token verification\nAge/identity check"| bankid
    drop -->|"AISP: GET /accounts\nAISP: GET /balances\nPISP: POST /payments"| nordic_banks
    drop -->|"PISP payment routing\nSEPA for EEA\nSWIFT for non-EEA"| payment_rails

    %% Compliance integrations
    drop -->|"Applicant creation\nDocument upload\nWebhook results"| sumsub
    drop -.->|"License registration\nRegulatory reporting\nCompliance audits"| finanstilsynet
    drop -.->|"STR filing\n(hvitvaskingsloven)"| okokrim

    %% Infrastructure
    drop -->|"Deploy containers\nAuto-scale"| aws
    drop -->|"DNS routing\nTLS, WAF\nDDoS protection"| cloudflare
    drop -->|"Error events\nPerformance traces"| sentry

    %% Bank to payment rails
```

```
    nordic_banks -->|"Execute transfers"| payment_rails

    classDef actorStyle fill:#E3F2FD,stroke:#1565C0,stroke-width:2px,color:#0D47A1
    classDef systemStyle fill:#0B6E35,stroke:#064E25,stroke-width:3px,color:#FFFFFF
    classDef bankingStyle fill:#FFF3E0,stroke:#E65100,stroke-width:2px,color:#BF360C
    classDef complianceStyle fill:#FCE4EC,stroke:#C62828,stroke-width:2px,color:#B71C1C
    classDef infraStyle fill:#F3E5F5,stroke:#6A1B9A,stroke-width:2px,color:#4A148C

    class sender,receiver,merchant actorStyle
    class drop systemStyle
    class bankid,nordic_banks,payment_rails bankingStyle
    class sumsub,finanstilsynet,okokrim complianceStyle
    class aws,cloudflare,sentry infraStyle
```

Trust Boundaries

```
graph TB
    subgraph tb_user["TRUST BOUNDARY: User Device (Untrusted)"]
        browser["Web Browser<br/>(Next.js SSR + CSR)"]
        mobile["Mobile App<br/>(Expo SDK 54)"]
    end

    subgraph tb_drop["TRUST BOUNDARY: Drop Application (Controlled)"]
        subgraph dmz["DMZ — Edge"]
            cf["Cloudflare<br/>WAF + CDN + DDoS"]
        end
        subgraph app["Application Layer"]
            nextjs["Next.js BFF<br/>Web auth, SSR"]
            hono["Hono API<br/>Mobile auth, REST"]
        end
        subgraph data["Data Layer"]
            pg["PostgreSQL<br/>(production)"]
            sqlite["SQLite<br/>(development)"]
        end
    end

    subgraph tb_banking["TRUST BOUNDARY: Banking Partners (External Trusted)"]
        bankid_tb["BankID OIDC"]
```

```
    openbanking["Open Banking APIs"]
end

subgraph tb_compliance["TRUST BOUNDARY: Compliance Partners (External Trusted)"]
    sumsub_tb["Sumsub KYC"]
end

subgraph tb_regulator["TRUST BOUNDARY: Regulatory (Government)"]
    fsa["Finanstilsynet"]
    efe["Okokrim / EFE"]
end

browser --> cf
mobile --> cf
cf --> nextjs
cf --> hono
nextjs --> pg
nextjs --> sqlite
hono --> pg
hono --> sqlite
nextjs --> bankid_tb
hono --> bankid_tb
nextjs --> openbanking
hono --> openbanking
nextjs --> sumsub_tb
hono --> sumsub_tb
nextjs -.-> fsa
nextjs -.-> efe

classDef untrusted fill:#FFCDD2,stroke:#C62828,stroke-width:2px
classDef controlled fill:#C8E6C9,stroke:#2E7D32,stroke-width:2px
classDef external fill:#FFF9C4,stroke:#F9A825,stroke-width:2px
classDef regulator fill:#E1BEE7,stroke:#6A1B9A,stroke-width:2px

class browser,mobile untrusted
class cf,nextjs,hono,pg,sqlite controlled
class bankid_tb,openbanking,sumsub_tb external
class fsa,efe regulator
```

External Actors

End Users

Actor	Description	Authentication	Data Exchanged
Sender	Norwegian resident (18+) who sends money abroad or pays merchants via QR	BankID OIDC (SCA)	Personal data, bank account info (AISP), payment instructions (PISP)
Receiver	Person in 30+ countries who receives remittance	None (indirect)	Receives bank transfer via payment rails
Merchant	Norwegian business accepting QR payments	BankID OIDC + merchant registration	Business details, org number, transaction data, payout info

Banking & Payment Systems

System	Protocol	Data Flow	Trust Level
BankID Norway	OIDC 2.0 (authorize, token, JWKS endpoints)	ID tokens with `pid` (national ID), name, DOB	High -- Norwegian government-backed eID
Nordic Banks (DNB, SpareBank1, Nordea)	PSD2 Open Banking REST APIs	AISP: account list, balances, transactions; PISP: payment initiation, status	High -- regulated financial institutions
SEPA (Single Euro Payments Area)	SEPA Credit Transfer (SCT)	EEA remittance transfers (1-2 business days)	High -- ECB-regulated
SWIFT	SWIFT gpi	Non-EEA remittance transfers (2-4 business days)	High -- SWIFT-regulated

Compliance & Regulatory

System	Integration	Data Flow	Cadence
Sumsub	REST API + Webhooks	Applicant data, document images, verification results, PEP/sanctions matches	On registration + ongoing monitoring
Finanstilsynet	Regulatory portal	License applications, compliance reports, incident notifications	Quarterly + ad hoc
Okokrim / EFE	AltInn reporting	STR/SAR filings per hvitvaskingsloven	As triggered by AML alerts

Infrastructure

System	Role	Protocol	Data Flow
AWS App Runner	Container hosting and auto-scaling	HTTPS, Docker	Application containers, environment variables, logs
Cloudflare	Edge security and CDN	DNS, HTTPS, WebSocket	HTTP traffic, TLS termination, DDoS filtering, WAF rules
Sentry	Error tracking and APM	HTTPS (SDK)	Error events, performance traces, session replays

---

Compliance Zone Mapping

PSD2 (Betalingstjenesteloven)

Requirement	Drop Component	External System	Status
Strong Customer Authentication (SCA)	Auth flow (`/api/auth/bankid/`)	BankID OIDC	Implemented
Dynamic linking (amount + payee tied to auth)	Payment confirmation screen	BankID SCA challenge	Phase 2
AISP consent and access	Bank account linking flow	Nordic bank Open Banking APIs	Phase 2
PISP payment initiation	Remittance + QR payment flows	Nordic bank Open Banking APIs	Phase 2
Framework agreement (vilkar)	`landing/pages/vilkar.html`	--	Draft exists
Pre-transaction fee disclosure	`POST /api/transactions/disclosure`	--	Implemented

GDPR (Personopplysningsloven)

Requirement	Drop Component	Implementation
Lawful basis for processing	`consents` table	Consent tracking with IP + timestamp
Right to access (Art. 15)	`GET /api/user/data-export`	Full data export in JSON
Right to erasure (Art. 17)	`DELETE /api/user/account`	Soft delete, 5yr AML retention
Data minimization (Art. 5)	Schema design	Only necessary fields stored

Requirement	Drop Component	Implementation
Data portability (Art. 20)	`GET /api/user/data-export`	Machine-readable JSON export
Processing register (Art. 30)	`data_access_requests` table	Tracks all DSAR requests
DPIA (Art. 35)	`legal/dpia-vurdering.md`	Draft completed

AML / KYC (Hvitvaskingsloven)

Requirement	Drop Component	External System
Customer Due Diligence (CDD)	User registration + KYC flow	Sumsub (document verification)
Enhanced Due Diligence (EDD)	`screening_results` table	Sumsub (PEP/sanctions screening)
Transaction monitoring	`aml_alerts` table	Internal rules engine
Suspicious Transaction Reporting	`str_reports` table	Okokrim / EFE via AltInn
Record keeping (5 years)	All compliance tables	PostgreSQL with retention policies
Risk assessment	`users.risk_level` field	Sumsub risk scoring

DORA (Digital Operational Resilience Act)

Requirement	Drop Component	Implementation
ICT risk management	`legal/ikt-sikkerhetspolicy.md`	Policy drafted
Incident reporting	`legal/hendelseshaandtering.md`	Incident handling procedure
Resilience testing	Planned penetration test	Phase 3
Third-party risk management	`legal/utkontraktering-policy.md`	Outsourcing policy drafted
Business continuity	`legal/beredskapsplan.md`	BCP drafted

Data Flow Summary

Flow	Source	Destination	Data	Protocol	Encryption
User authentication	Browser/Mobile	BankID	OIDC auth request, state, nonce	HTTPS	TLS 1.3
Identity verification	Drop	BankID	Authorization code exchange	HTTPS	TLS 1.3
Balance read (AISP)	Drop	Nordic Bank	Account ID, consent token	PSD2 Open Banking API	TLS 1.3 + OAuth2

Flow	Source	Destination	Data	Protocol	Encryption
Payment initiation (PISP)	Drop	Nordic Bank	Amount, recipient, consent	PSD2 Open Banking API	TLS 1.3 + OAuth2 + SCA
KYC verification	Drop	Sumsub	Applicant data, documents	REST API + Webhooks	TLS 1.3 + API key
STR filing	Drop	Okokrim	Suspicious transaction report	AltInn portal	TLS 1.3 + certificate
Error tracking	Drop	Sentry	Error events, stack traces	HTTPS SDK	TLS 1.3 + DSN token
Web traffic	User	Cloudflare -> Drop	HTTP requests/responses	HTTPS	TLS 1.3 (edge + origin)

Cross-References

- Container Diagram (C4 Level 2) -- Internal container breakdown
- Security Architecture -- Detailed security controls
- BankID OIDC Integration -- Authentication integration spec
- Open Banking AISP/PISP -- Banking integration spec
- Sumsub KYC Integration -- KYC provider integration
- ADR-003: PSD2 Pass-through Model -- Foundational architecture decision
- ADR-007: BankID OIDC Auth -- Authentication provider decision

Revision #7
Created 2026-02-21 05:58:47 UTC by John
Updated 2026-05-23 10:51:30 UTC by John