FinSecure Payment Platform

Technical Architecture Document v3.2
Classification: Internal - Confidential

1. Executive Summary

FinSecure is a PCI-DSS Level 1 compliant payment processing platform handling over $2.5B in annual transaction volume. The platform provides real-time payment processing, fraud detection, and merchant services through a microservices architecture deployed on AWS with multi-region failover capabilities.

2. System Architecture Overview

The platform follows a layered microservices architecture with clear separation between external-facing components (DMZ), core business services (Application Layer), and sensitive data stores (Data Layer). All inter-service communication uses mTLS with certificate rotation every 90 days.

2.1 Core System Components

Component	Technology	Description	Security Controls
API Gateway	Kong Enterprise	Entry point for all external API traffic	WAF, Rate limiting, JWT validation
Identity Service	Keycloak + Custom	OAuth2/OIDC provider with MFA	HSM-backed keys, Session management
Payment Orchestrator	Java 17 / Spring Boot	Core payment routing and processing	PCI-DSS scope, Tokenization
Fraud Detection Engine	Python / TensorFlow	ML-based real-time fraud scoring	Anomaly detection, Risk scoring
Card Vault	Custom C++ / HSM	PAN storage and tokenization	HSM integration, P2PE encryption
Ledger Service	Go / CockroachDB	Double-entry accounting system	Immutable audit log, Reconciliation
Notification Hub	Node.js / Kafka	Multi-channel notifications	Template injection prevention
Merchant Portal	React / Next.js	Merchant self-service dashboard	CSP headers, XSS protection

2.2 Critical Data Flows

1. Payment Authorization Flow:

Merchant POS → API Gateway (TLS 1.3) → Payment Orchestrator → Card Vault (HSM decrypt) → Card Network → Response

2. User Authentication Flow:

Mobile App → CDN → API Gateway → Identity Service → User DB (bcrypt) → JWT issued → Redis session

3. Fraud Detection Flow:

Transaction Event → Kafka → Fraud Engine (ML inference) → Risk Score → Payment Orchestrator → Approve/Decline

4. Settlement Flow:

Batch Job (2AM UTC) → Ledger Service → Settlement calculations → ACH/Wire submission → Bank API

3. Trust Boundaries & Network Segmentation

Zone	Components	Network	Access Control
Internet (Untrusted)	CDN, WAF	Public IPs	DDoS protection, Geo-blocking
DMZ	API Gateway, Load Balancers	10.1.0.0/24	Ingress firewall, IDS/IPS
Application Zone	All microservices	10.2.0.0/16	Service mesh (Istio), mTLS
PCI Zone (CDE)	Card Vault, Payment Orch.	10.3.0.0/24	HSM, Network isolation, MFA
Data Zone	Databases, Caches	10.4.0.0/24	Encryption at rest, VPC endpoints
Management Zone	Bastion, Monitoring	10.5.0.0/24	MFA + VPN required

4. External System Integrations

• **Card Networks:** Visa (VTS), Mastercard (MDES), Amex - Direct API integration with dedicated circuits

• **Banking Partners:** Wells Fargo (ACH), JP Morgan (Wire transfers) - SFTP with PGP encryption

• **KYC/AML Providers:** Jumio (Identity verification), LexisNexis (Watchlist screening)

• **Cloud Services:** AWS (Primary), Azure (DR), Cloudflare (CDN/DDoS)

• **Monitoring:** Datadog (APM), PagerDuty (Alerting), Splunk (SIEM)

5. Security Architecture

5.1 Authentication & Authorization

• OAuth 2.0 with PKCE for all client applications • Hardware MFA (FIDO2/WebAuthn) required for privileged access • Service-to-service auth via mTLS with short-lived certificates (Vault PKI) • Role-Based Access Control (RBAC) with principle of least privilege • Session timeout: 15 minutes idle, 8 hours absolute

5.2 Data Protection

• PAN tokenization using format-preserving encryption (FPE) • All PII encrypted at rest using AES-256-GCM (AWS KMS) • TLS 1.3 enforced for all external connections • Database field-level encryption for sensitive columns • Key rotation: 90 days for service keys, annual for master keys

5.3 Logging & Monitoring

• Centralized logging with 7-year retention (PCI requirement) • Real-time anomaly detection on authentication events • Transaction monitoring with velocity checks • Automated incident response playbooks • Quarterly penetration testing by third party

6. Data Architecture

Database	Type	Data Classification	Encryption
card_vault_db	PostgreSQL (RDS)	PCI - Cardholder Data	TDE + Column-level
user_identity_db	PostgreSQL (RDS)	PII - Personal Data	TDE + Field encryption
transaction_ledger	CockroachDB	Financial Records	TDE
fraud_features	Redis Cluster	Derived Data	In-transit only
audit_logs	Elasticsearch	Security Logs	TDE
merchant_config	DynamoDB	Configuration	AWS managed