FINOVAMAX SECURITY WHITE PAPER

Security at the Centre of Core Banking

How FinovaMax protects customer data and institutional integrity — for the security and compliance teams evaluating it.

Version **1.0** 21 June 2026 Apex Grid Technologies Ltd · RC 9108833 · Lagos & Abuja, Nigeria

This paper describes **implemented controls**. Where it references PCI DSS or ISO 27001, it describes engineering *against* those standards and the audit path ahead — not certifications currently held (see §10). Where deeper implementation detail is referenced as available under NDA, that detail is shared during a formal evaluation.

Contents

1. Executive summary

FinovaMax is core-banking software engineered so that security and regulatory control sit at the centre of the platform rather than bolted on at the edges. This paper documents the controls that protect customer data and institutional integrity across every layer — data at rest, identity and access, the application and API surface, multi-tenant isolation, audit evidence, and the privacy obligations Nigerian institutions carry.

The guiding principle is **defence in depth**: no single control is load-bearing on its own. Encryption protects data at rest; tenant isolation contains blast radius; an immutable audit log makes every action provable; and privacy controls enforce data-subject rights and breach-notification deadlines as platform behaviour, not policy documents.

2. Security architecture & principles

- **Compliant-by-design.** The compliance and security engine is central to the platform; loans, savings, payments, and mobile connect through it rather than around it.
- **Defence in depth.** Controls are layered across the edge, application, data, and audit tiers so that the failure of any one control does not expose customer data.
- **Least privilege.** Access — human and programmatic — is scoped to what each role or integration needs (see §4 and §5).
- **Secure by default.** Core protections are enabled per tenant without requiring the institution to configure them on.
- **Tenant isolation as a first-class property.** Each institution's data is logically isolated and enforced at the data and query layer (see §6).

3. Data protection (encryption at rest & in transit)

- **Encryption at rest.** Versioned AES-256-GCM encryption with automated key rotation across 130+ columns and 40+ tables, implementing PCI DSS 3.6.3 key-rotation requirements. Sensitive identifiers (BVN, NIN, PAN, and similar) are encrypted at the field level.
- **Encryption in transit.** All data in transit — browser, API, and inter-service — is protected with TLS.
- **Key management.** Encryption keys are versioned and rotated automatically, so a rotation does not require re-encrypting or taking the platform offline. Key-custody and rotation-cadence specifics are provided under NDA during evaluation.

4. Identity & access management

- **Two-factor authentication.** TOTP authenticator-app 2FA with backup codes, per-institution enforcement, anti-replay protection, and role-based mandates.
- **Session security to PCI DSS 8.1.8.** Configurable idle timeout, JWT rotation, and account-lockout policies.
- **Role-based access control.** Permissions follow least-privilege; administrative actions are constrained and recorded in the audit log (§7).

5. Application & API security

The Public API is a standalone service built for partner banks, fintechs, and third-party integrations:

- **HMAC-SHA256 authentication** with timestamped, signed requests.
- **17 granular scopes**, and two access tiers: *tenant:own-data* (full access) and *third-party:query* (masked BVN/NIN).
- **SSRF prevention, constant-time key validation, rate limiting, and CSRF double-submit cookies.**
- **Webhooks** with HMAC-signed delivery and exponential-backoff retry.
- **Full audit logging** of API activity (§7) and input validation across endpoints.

6. Multi-tenant isolation

- **Logical isolation** is enforced at the data and query layer, so one institution can never reach another's data.
- **Per-tenant configuration** — limits, thresholds, enforcement policies, and hosting jurisdiction — is scoped to the individual institution.
- The isolation model and its testing approach are detailed under NDA during a security evaluation.

7. Immutable audit trail

- **Hash-chain audit log** for every action — login, transaction post, compliance-case decision, configuration change, administrator action. Each entry contains the hash of the previous entry, so silently altering an earlier entry breaks the chain visibly.
- **Full context per entry:** actor (user ID), action, affected record, timestamp, source IP, and user-agent.
- **Ten-year retention** by default, matching regulatory expectation.
- **Examiner-ready exports** direct from the platform, not a curated extract.

8. PII protection & data minimisation

- **PII log sanitiser** — automatic masking of BVN, NIN, PAN, and JWT tokens in all log output, so sensitive identifiers never leak to monitoring systems.
- **Separation of audit vs operational logs** — operational telemetry is sanitised; the evidentiary audit log (§7) is preserved in full.
- **Biometric data minimisation** — KYC biometric capture is purged from the device after submission, in line with the NDPA's data-minimisation principles.

9. Data privacy controls (NDPA 2023 / GAID)

Data protection in Nigeria is governed by the Nigeria Data Protection Act (NDPA) 2023, read together with the NDPC's General Application and Implementation Directive (GAID), which superseded the NDPR 2019 with effect from 19 September 2025. FinovaMax implements the relevant obligations as platform behaviour:

- **Data-subject rights (NDPA §§34–38)** — access, rectification, restriction, objection, and portability requests routed to an operator queue with SLA tracking and DPO sign-off, and enforced in downstream queries so withdrawn-consent records stay out of reports.
- **Breach notification (NDPA §40)** — an incident registry with a built-in 72-hour NDPC notification-deadline tracker, severity scoring, affected-records counting, and resolution timeline.
- **DPO & registration (NDPA §32 / §44)** — DPO record management and NDPC registration details, plus per-tenant sub-processor disclosure tracking under the Act's data-processor obligations and the GAID.

Official text: NDPC — Nigeria Data Protection Act 2023.

10. Certification posture

- FinovaMax is **engineered against PCI DSS v4.0 and ISO 27001:2022 control standards today** — controls implemented, not yet certified.
- The formal **QSA-led audit and certification path is co-timed with the founding customer's go-live**: that production environment becomes the certified reference architecture for the public certification statement.
- This paper does not state or imply current certification — only engineering against the standards and a scheduled audit path.

11. Hosting, data residency & resilience

- **Residency-ready architecture** — designed to deploy on Nigerian-resident infrastructure, with per-tenant hosting jurisdiction configurable. This aligns with the CBN's payment-data-localisation directive (Circular PSS/DIR/PUB/CIR/001/004, effective 1 January 2027).
- **Backups & recovery** — data is backed up on a defined rotation with encryption, supported by disaster-recovery procedures. Recovery objectives are agreed per deployment and detailed under NDA.
- **Jurisdiction-agnostic data model** — moving the data location does not require changing the data model, so on-shore migration is a hosting decision, not a re-platforming project.

12. Scope of claims

To keep this paper trustworthy with a security-literate audience, FinovaMax states its position precisely:

- No current PCI DSS or ISO 27001 certification is claimed — only engineering against the standards and a scheduled audit path (§10).
- Integrations are described as built / pre-built, with activation at customer go-live; no third-party "live" status is implied.
- Numeric figures (e.g. 130+ columns, 40+ tables, 17 API scopes, ten-year retention) are stated only where verifiable.
- Implementation specifics noted as "under NDA" are disclosed during a formal evaluation rather than asserted publicly.

13. Appendix

Control-to-standard mapping

Control	Reference
AES-256-GCM encryption & automated key rotation	PCI DSS 3.6.3
Session idle timeout, JWT rotation, account lockout	PCI DSS 8.1.8
TOTP two-factor authentication	PCI DSS / ISO 27001 access-control families
Immutable hash-chain audit log, 10-year retention	CBN Risk-Based Cybersecurity Framework; NDPA evidentiary expectations
Data-subject rights workflows	NDPA 2023 §§34–38
Breach incident registry (72-hour clock)	NDPA 2023 §40
DPO & registration records	NDPA 2023 §32, §44
Data residency / per-tenant hosting jurisdiction	CBN Circular PSS/DIR/PUB/CIR/001/004 (eff. 1 Jan 2027)

Glossary

AES-256-GCM	Authenticated symmetric encryption algorithm used for data at rest.
BVN / NIN / PAN	Bank Verification Number; National Identification Number; Primary Account Number.
CSRF	Cross-Site Request Forgery — mitigated here with double-submit cookies.
GAID	General Application and Implementation Directive issued by the NDPC under the NDPA 2023.
HMAC-SHA256	Keyed-hash message authentication used for API request signing.
JWT	JSON Web Token — session/credential format, rotated per policy.
NDPA / NDPC	Nigeria Data Protection Act 2023 / Nigeria Data Protection Commission.
PCI DSS	Payment Card Industry Data Security Standard (v4.0 referenced).
QSA	Qualified Security Assessor — conducts the formal PCI DSS audit.
SSRF	Server-Side Request Forgery — prevented at the API layer.
TOTP	Time-based One-Time Password — the 2FA mechanism.

TLS	Transport Layer Security — encryption for data in transit.