Generated on 8/14/2025

DVPATS- Technical Spec

Security Assessment Report

1. Baseline Assessment

Business Importance
Stride Electronics is a dual-sided online marketplace for electronics with social features. It manages payments, commissions, a credit wallet, seller KYC verification, and an admin panel. The platform is **business-critical** due to handling of payments, PII, and compliance obligations (**GDPR, PCI-DSS**).

Document Coverage

- **Strengths:** Clear technical components (frontend, backend, APIs), third-party integrations (payments/KYC), and data flows.
- **Security Mentions:** HTTPS/TLS, OAuth 2.0, JWTs, PCI references, KYC workflows.
- **Gaps:** No concrete detail on **MFA, RBAC, session lifecycle, API rate limiting/anti-bot, KYC encryption/retention, audit logging/monitoring, PCI scoping**.

Design Document Ratings (1–10):

- **Security Information:** 4 — Mentions standards but lacks control specifics.
- **Technical Depth:** 6 — Strong on systems/APIs; light on security operations and governance.
- **Business Criticality:** 9 — Directly tied to revenue, fraud exposure, and compliance posture.

2. Asset Inventory

Sensitive Assets

- User PII (profiles, addresses, order history)
- Authentication tokens (JWTs, OAuth refresh tokens)
- Payment tokens/transaction metadata

- StrideCredit balances & refund history
- Seller KYC documents & verification status
- Admin actions & approval records (payouts, KYC, bans)

Non-Sensitive Assets

- Product/catalog metadata & images
- Public social interactions (likes, comments, follows)
- Notification preferences

3. Component Inventory

- **Frontend:** Next.js/React web & mobile clients
- **APIs/Services:** Auth, Catalog, Orders/Payments, Wallet, Notifications, Admin
- **Integrations:** PCI payment gateway, KYC provider, Email/SMS
- **Data Stores:** Relational DB (PII/metadata), object/file storage (uploads)
- **Edge/Infra:** HTTPS LB/API gateway, app servers, monitoring stack (not specified)

4. Concise Security Review

Overall Risk Rating: HIGH

1. **Token/Sessions:** JWT expiry/rotation undefined; refresh handling and cookie flags unspecified.
2. **Access Control:** RBAC granularity for Admin Panel not documented; MFA not mandated for admins.
3. **API Abuse:** No rate limiting/anti-automation on login, wallet, search; scraping and brute force likely.
4. **KYC Protection:** Storage encryption, access controls, and retention/deletion not defined.
5. **Monitoring/Audit:** No audit events or SIEM integration for high-risk operations (payouts, KYC access).
6. **PCI Scope:** Payment provider used, but architectural scoping and “no PAN ever touches the app/logs” not explicit.

5. Confirmed Threats & Mitigations

Threat	Severity	Description	Mitigation
JWT Misuse & Replay	**High**	Long-lived/poorly validated JWTs enable session hijack or replay across services.	Short JWT TTLs; rotate on login/priv-change; strict iss/aud checks; revoke on password reset; bind tokens to client context.
Admin Privilege Escalation	**Critical**	Broad Admin Panel powers (payouts, KYC, bans) with unclear RBAC allow outsized impact if compromised.	Least-privilege RBAC; mandatory **MFA**; just-in-time elevation; dual-control for payouts/KYC; immutable audit trails.
StrideCredit Fraud/Abuse	**High**	Refund loops/partial redemptions without velocity caps enable financial abuse.	Velocity/amount caps; redemption limits per order/day; anomaly detection; manual reviews; tamper-evident ledgers.
KYC Document Exposure	**Critical**	Identity scans stored without explicit encryption/retention/access controls risk breach & regulatory action.	Encrypt at rest; segregated storage; ABAC on views; redaction for support; retention/deletion SLAs; access telemetry.
API Brute Force & Enumeration	**High**	Login/reset/search endpoints lack throttling; credential stuffing & scraping likely.	Per-IP/user rate limits; CAPTCHA on anomalies; device reputation; error messages that avoid user enumeration.
Weak Monitoring/Forensics	**High**	No defined audit events/SIEM; insider or external abuse may go undetected.	Audit admin actions, payouts, KYC views, failed logins; centralize to SIEM; alert on abnormal patterns.

PCI DSS Scope Creep	**Critical**	Ambiguous scoping risks PAN entering app/logs; compliance failure possible.	Hosted fields/iFrames; tokenize with PCI provider; block PAN in logs; network segmentation; formal SAQ/ROC.
Session Lifecycle Weakness	**High**	Idle/absolute timeouts and cookie flags (Secure/HttpOnly/SameSite) not defined; increases hijack risk.	Idle (15–30m) & absolute (≤24h) timeouts; rotation on privilege change; `Secure`/`HttpOnly`/`SameSite=Strict/Lax` cookies; global logout.

6. Open Questions

Authentication & Identity

- Will **MFA** be **mandatory for admin accounts** and available/required for high-risk user actions (payouts, address/bank updates)?
- How is **social login linking** protected (re-authentication, email proof, notifications on link)?
- What **password hashing** (e.g., Argon2/bcrypt with parameters) is defined for native accounts?

Session & Token Management

- Exact **JWT TTLs** (idle and max/absolute)? Do we **rotate** on login and privilege change?
- **Refresh token** storage/rotation strategy and **revocation** on logout or suspected compromise?
- **Cookie flags**: `Secure`, `HttpOnly`, `SameSite` settings across web flows; CSRF protections for state-changing endpoints?

API & Abuse Protection

- **Rate-limiting thresholds** for **login**, **password reset**, **search**, **wallet/credit**, and **payout** APIs (per IP/user/device)?
- Any **anti-bot** controls (proof-of-work, device fingerprinting, behavior signals) at auth and checkout?
- **Input validation/schema enforcement** (server-side) for product descriptions, comments, images, and prices?

Data Protection & Compliance

- **KYC storage**: where (object store/DB), which **encryption (KMS/keys, rotation)**, and **who** can access (ABAC/RBAC)?
- **Retention/deletion** SLAs for **KYC** and **order data**; data minimization strategy for logs/backups?
- **GDPR/DSR**: process/SLA for access, deletion, and export; data lineage for locating PII across services.
- **PCI boundaries**: precise **data-flow** showing card data never touches app/DB/logs; target **SAQ level** and compensating controls.

Monitoring, Audit & Incident Response

- **Audit events** to log: admin role changes, payouts, KYC views/decisions, credit adjustments, suspicious logins.
- **SIEM integration**: pipeline, alert rules, on-call ownership; **retention** and **tamper-evidence** for logs.
- **IR playbooks**: criteria for account lock, token revocation, and payout holds; escalation timelines/owners.

App/Content Security

- **CSP** policy (script/img/connect directives), **HTML sanitization** for UGC, and **image/file scanning** (MIME/type/AV).
- **CSRF** protections on state-changing endpoints; **CORS** policy for APIs; download tokenization for invoices.

Secrets, Backups & Resilience

- **Secrets management** (KMS/secret store), rotation cadence, and prevention of secret leakage in logs.
- **Backup/restore** encryption and access controls; **RPO/RTO** and key recovery for encrypted data.

Network/Edge

- **WAF/DDoS** strategy at the edge; bot management; IP reputation lists.
- **Service segmentation/zero-trust** between services handling sensitive data (Auth/Payments/KYC).