

TrustBridge MVP – Cybersecurity Strategy

Our security design ensures TrustBridge is not just functional, but **institution-grade and NDPR-aligned**, even within a 3-week MVP timeline.

1. Supabase Security Configuration

Built on Supabase (PostgreSQL + Auth + Storage).

Row-Level Security (RLS) – Mandatory

- Enabled on all tables: users, business_profiles, transactions, transaction_proofs
- SMEs can only access their own records using:
 - USING (auth.uid() = owner_id);

Service Role Protection

- Service role key never exposed to frontend
- Stored only in backend environment variables (Vercel / .env)

Secure File Storage

- Proof uploads stored in **private buckets**
- Access via signed URLs only
- No public file links

Auth Hardening

- Email verification enabled
- Anonymous sign-ins disabled
- Short-lived access tokens
- Refresh token rotation enabled

Database Controls

- Foreign key enforcement
- Indexed critical fields (owner_id, transaction_id)
- Daily backups + audit logs

- Parameterized queries to prevent SQL injection
-

2. Secure Confirmation Link (JWT-Based)

This protects against:

- Link guessing
- Replay attacks
- Link tampering
- Unauthorized confirmations

Flow:

1. SME marks job as delivered
2. Backend generates **signed JWT (72-hour expiry)**
3. Client receives:
4. <https://trustbridge.app/confirm?token=...>

JWT Contains:

- txn_id
- client_email
- action: confirm
- exp (72 hours)

On Link Click:

- Verify signature
- Check expiry
- Confirm transaction status
- Mark as “Verified”

Extra Protections:

- One-time-use token (stored as hash in DB)
- Token marked as used after confirmation

- Confirmation IP + timestamp logged

Don'ts: expose transaction details in URLs
use unsigned or predictable links

3. Data Encryption Standards (MVP)

Encryption in Transit

- HTTPS only (TLS 1.2+)
- HSTS via Vercel

Encryption at Rest

- Supabase DB & Storage encrypted
- Sensitive fields protected
- Optional hashing of client emails (SHA-256)

Password Security

Handled by Supabase Auth (bcrypt hashing).

No plaintext passwords stored.

Key Management

- Secrets in environment variables
 - No hardcoded keys
 - No secrets committed to Git
-

4. NDPR Alignment

Aligned with Nigeria's NDPR principles:

- Data minimization
- Explicit client consent before confirmation
- Privacy notice
- "Delete Account" capability

TrustBridge collects only what is necessary for trust verification.

5. MVP Security Protocol

Threat Model & Mitigation

Threat	Mitigation
Account takeover	Email verification
Data scraping	RLS policies
Link tampering	Signed JWT
Replay attack	One-time tokens
File abuse	File validation + size limits
XSS	Input sanitization
CSRF	SameSite cookies

Secure Coding Rules

Frontend

- Validate file types
- Limit uploads ($\leq 5\text{MB}$)
- Escape user inputs

Backend

- Validate all inputs
 - Never trust frontend validation
 - Use parameterized queries
-

Logging & Monitoring

Track:

- Login attempts
- Failed confirmations
- Token misuse
- Suspicious IPs

Supabase logging is sufficient for MVP scale.

6. 3-Week Execution Plan

Week 1:

RLS policies, storage security, auth hardening

Week 2:

JWT confirmation system + encryption standards

Week 3:

Internal penetration testing:

- Broken access control
- URL tampering
- SQL injection
- File abuse

Document findings for judges.

What This Signals to Judges

TrustBridge is built with:

- Row-Level Security
- Encrypted data (at rest & in transit)
- Time-bound JWT confirmation links
- One-time verification tokens
- NDPR-compliant privacy design

This positions TrustBridge as a **secure digital trust infrastructure** for informal economies, not just a prototype.
