TrustBridge Secure Confirmation Link – JWT Technical Specification v1.0

Prepared by: Cybersecurity Team

Project: TrustBridge MVP

1. Objective

This document defines the technical implementation of secure confirmation link generation using JSON Web Tokens (JWT) to prevent fraud, replay attacks, and trust score manipulation.

2. Token Generation Process

When an SME uploads proof and marks a transaction as delivered:

1. Backend generates a JWT containing:

- transaction_id
- issued_at timestamp (iat)
- expiration timestamp (exp = current time + 72 hours)
- random nonce value

2. Token is signed using a secure server-side secret (HS256 or RS256).

3. Token is stored in hashed form in the database.

4. Confirmation link is generated as:

https://trustbridge.com/confirm?token=<JWT>

3. Token Validation Process

When client clicks confirmation link:

1. Server verifies JWT signature.

2. Server checks token expiration.

3. Server verifies token has not been used.

4. If valid, transaction status updates to 'Verified'.

5. Token is immediately invalidated (single-use enforcement).

4. Security Controls Implemented

- Cryptographically secure random nonce prevents predictability.
- Expiration window (72 hours) reduces replay risk.
- Single-use enforcement prevents duplicate confirmations.
- Signature validation prevents tampering.
- Row-Level Security ensures only authorized transaction is updated.

5. Threats Mitigated

- Link guessing or brute-force attacks
- Replay attacks
- Token tampering
- Fraudulent trust score inflation

6. Recommended Implementation (Node.js Example)

Use jsonwebtoken library:

```
const jwt = require('jsonwebtoken');
const token = jwt.sign(
  { transaction_id: id },
  process.env.JWT_SECRET,
  { expiresIn: '72h' }
);
```