Company	AcmeTech Solutions Pvt. Ltd.	Assets Scanned	18
Sector	Financial Technology	Report Version	1.0
Scan Date	June 2026	Classification	Confidential
Prepared by	Novaders LLP — dinesh@novaders.com		

RISK SUMMARY

3 CRITICAL — Action before 2028

2 HIGH — Action before 2030

1 MEDIUM — Monitor

12 SAFE — No action needed

TOP FINDINGS

#	ASSET	RISK	REPLACE WITH	STANDARD	EFFORT
1	**payments-api** RSA-2048 encryption	CRITICAL	ML-KEM-768	FIPS 203	Medium
2	**auth-service** ECDSA P-256 signing	CRITICAL	ML-DSA-44	FIPS 204	Medium
3	**cert-01, cert-02, cert-03 (internal PKI)** RSA-2048 certificates	CRITICAL	ML-DSA hybrid cert	FIPS 204	High
4	**api.acmetech.com** TLS 1.2 — RSA key exchange	HIGH	TLS 1.3 + X25519/ML-KEM-768	FIPS 203	Low
5	**14 SSH keys (infra)** RSA-2048 SSH keys	HIGH	Ed25519 (immediate)	—	Low
6	**user-data-service** AES-128 encryption	MEDIUM	AES-256	—	Low
7	**document-store** HMAC-SHA256	SAFE	No action	—	—

⚠ **HARVEST NOW, DECRYPT LATER RISK DETECTED** — The 3 CRITICAL assets handle financial transaction data with retention periods exceeding 10 years. This data is at risk of being captured today and decrypted once quantum computers become available. Immediate migration planning is recommended.

PRIORITISED MIGRATION ROADMAP

Mapped to NIST IR 8547 deprecation timelines. Recommended approach: hybrid migration (classical + PQC in parallel).

PHASE 1 — IMMEDIATE (2026)

▸ Rotate 14 SSH keys
RSA-2048 → Ed25519
Effort: Low — 1 day

▸ Upgrade TLS on api.acmetech.com
Add hybrid PQC extension
Effort: Low — config change

PHASE 2 — SHORT-TERM (2026–2027)

▸ Migrate payments-api
RSA-2048 → ML-KEM-768 (FIPS 203)
Effort: Medium — library swap

▸ Migrate auth-service
ECDSA P-256 → ML-DSA-44 (FIPS 204)
Effort: Medium — library swap

▸ Upgrade AES-128 to AES-256
user-data-service
Effort: Low — config change

PHASE 3 — MEDIUM-TERM (2027–2028)

▸ Reissue 3 internal certificates
RSA-2048 → ML-DSA hybrid cert
Effort: High — PKI migration

▸ Validate all migrated services
Full post-migration audit
Effort: Medium

RECOMMENDED: HYBRID MIGRATION — Do not hard-cut from classical to PQC. Run both algorithms in parallel (e.g. X25519 + ML-KEM-768) during the transition window. This is the approach used by Cloudflare, Google, and Apple in production today. Novaders will configure and validate hybrid mode for each migrated service.

TOTAL MIGRATION EFFORT ESTIMATE

CATEGORY	ITEMS	ESTIMATED EFFORT
Library / code changes	2 services	3–5 weeks (engineering)
Configuration changes	3 items	2–4 days (DevOps)
Certificate reissuance	3 certs	1–2 weeks (PKI team)
SSH key rotation	14 keys	1 day (ops)
Total	**18 assets**	**~6–8 weeks total**

ABOUT THIS ASSESSMENT

WHAT WAS SCANNED

- ✓ Source code repositories (GitHub)
- ✓ Package dependency manifests
- ✓ Public TLS certificates and cipher suites
- ✓ SSH key inventory
- ✓ API endpoint handshake inspection
- × Binary / compiled artefacts (out of scope)
- × Hardware security modules (out of scope)

STANDARDS REFERENCED

- **NIST FIPS 203** — ML-KEM (Key Encapsulation)
- **NIST FIPS 204** — ML-DSA (Digital Signatures)
- **NIST FIPS 205** — SLH-DSA (Hash-based Signatures)
- **NIST IR 8547** — Migration timelines
- **CISA PQC Migration Guidance** (2024)