LATTICA AUDIT PACK

Executive summary

acme-payments/api-gateway

CycloneDX 1.6 · Scanned 2026-06-15T09:00:00Z · 104 rules · sha256 9f2c1ea7b4d05583cf0a1d6e

Findings by severity

CRITICAL	HIGH	MEDIUM	LOW	INFO
14	41	88	63	12

Coverage

Total findings: 218
Cryptography findings: 190
Quantum-software findings: 28

Mandatory & regulatory triggers

PCI-DSS 4.0.1 — **Req 12.3.3 — Cryptographic Cipher Inventory**
Mandatory since 31 Mar 2025: maintain a documented inventory of cryptographic ciphers/protocols in use, with a migration plan. This CBOM is that inventory.

FIPS 140-2 — **Validated-Module Transition**
FIPS 140-2 modules move to the NIST Historical List on 21 Sep 2026; procurements increasingly require FIPS 140-3 + PQC-readiness. Inventory classical usage now.

CNSA 2.0 — **Commercial National Security Algorithm Suite**
U.S. national-security & federal-adjacent systems: ML-KEM-1024 + ML-DSA-87 + AES-256 + SHA-384; software/firmware procurement gates begin 1 Jan 2027.

FIPS 203 — ML-KEM — **Module-Lattice Key Encapsulation**
Migrate RSA-KEM and ECDH KEM consumers to ML-KEM-768 (Cat 3) or ML-KEM-1024 (Cat 5).

FIPS 204 — ML-DSA — **Module-Lattice Digital Signature**
Migrate RSA-PKCS1, RSA-PSS, ECDSA, and EdDSA signers to ML-DSA-44 / 65 / 87.

FIPS 205 — SLH-DSA — **Stateless Hash-Based Signature**
Acceptable fallback for low-frequency long-lived signatures (firmware, root CAs).

NIST SP 800-208 — **Stateful Hash-Based Signatures**
LMS / XMSS for transitional code-signing where ML-DSA is not yet available.

EU eIDAS 2.0 — **Trust Services PQC Alignment**
Trust-service providers must publish PQC roadmaps; guidance issued 2025.

Methodology & limitations

This Audit Pack reports the cryptographic-asset inventory found by lattica-scan against the indicated source. It maps each detected primitive to NIST FIPS 203 / 204 / 205 (ML-KEM, ML-DSA, SLH-DSA) and to the regulatory triggers listed on page 1.

Scope: lattica-scan inspects source code and configuration files (key generation, classical TLS configs, JWT algorithms, keystores, and cert/key files). It is a source-and-configuration inventory — it does not introspect running infrastructure, HSMs, cloud KMS, container images, or compiled binaries. Findings include file path, line number, rule ID, and severity. The CycloneDX 1.6 CBOM artifact (sha256 on page 1) is the canonical evidence.

Limitations: detection is rule-based and may report false positives (test fixtures, intentionally-pinned legacy crypto) and false negatives (highly dynamic code paths, unparsed binaries). This document supports a Req 12.3.3 cryptographic inventory and PQC-readiness planning; it is not a SOC 2 audit opinion or legal advice.

Recommended use: include this pack with your internal control documentation, hand it to your QSA / auditor / GRC platform alongside the CBOM artifact, and use the prioritized severity bands to plan remediation. The HNDL methodology (lattica.dev/threat-clock) provides per-endpoint risk scoring when endpoint context is supplied.

LATTICA AUDIT PACK

Post-Quantum Migration Status

How much of your detected cryptography is already quantum-resistant.

15% post-quantum

29 post-quantum vs 161 classical quantum-vulnerable detections

Post-quantum — in place

- **Key encapsulation — ML-KEM / Kyber**
  18x · FIPS 203 — quantum-resistant
- **Signatures — ML-DSA / SLH-DSA / Falcon**
  6x · FIPS 204 / 205 — quantum-resistant
- **TLS key exchange — hybrid (X25519MLKEM768)**
  3x · recommended transitional posture
- **Post-quantum library present (liboqs / CIRCL / noble)**
  2x · inventory

Still classical — migrate

- **RSA**
  72x -> migrate to ML-KEM (KEM) / ML-DSA (sign)
- **ECC / ECDSA / ECDH**
  54x -> migrate to ML-KEM / ML-DSA
- **Diffie-Hellman**
  12x -> migrate to ML-KEM
- **Classical JWT (RS256 / ES256)**
  14x -> migrate signing to ML-DSA
- **Classical TLS ciphers**
  9x -> enable hybrid PQC key exchange

Verdict: post-quantum adoption is underway and hybrid key exchange is present. Complete the migration by replacing the remaining classical signing and transport listed above.

Scope & Methodology

What this scan covered, what it did not, and how the inventory was produced.

Scanned

Automated rule-based (regex) detection over the source code and configuration of acme-payments/api-gateway. Coverage spans 7 languages (Go, TypeScript/JavaScript, Java, Python, Rust, C/C++, C#) and common config (TLS, JWT, keystores, cert/key files).

FILES SCANNED	**3,142**
BYTES SCANNED	**27.3 MB**
RULESET	**104 rules**
LANGUAGES COVERED	**7**
SUBJECT	**acme-payments/api-gateway**
DETECTION	**automated rule-based (regex) over source + config**

Not covered

- Runtime / in-memory cryptography (only code and config on disk are inspected).
- HSM- or TPM-resident keys and their algorithms.
- Cloud KMS-managed keys (AWS KMS, GCP KMS, Azure Key Vault, etc.).
- Compiled binaries, container images, and other non-source artifacts.
- Certificate estate and live TLS endpoints, unless separately inventoried with lattica-certs / lattica-tls.
- Taint, data-flow, and reachability analysis (detection is call-level, not whole-program).

Rule-based detection carries false-positive risk (test fixtures, intentionally-pinned legacy crypto) and false-negative risk (highly dynamic code, unparsed artifacts). Results are point-in-time.

Methodology

Rule-based scan -> human review of findings -> CycloneDX 1.6 CBOM artifact. Coverage can be widened with AST-based detection (call-resolved, reduces false positives), a lattica-certs inventory (certificate / PKI estate), and a lattica-tls inventory (live endpoint cipher and key-exchange posture).

Verdict: this is an inventory artifact that supports - and does not replace - the organization's own cryptographic inventory and PQC-migration program.

LATTICA AUDIT PACK

Cryptographic Inventory Summary

ILLUSTRATIVE SAMPLE · synthetic data · not a real scan or a valid summary

This is a self-issued, point-in-time Cryptographic Inventory Summary — not a PKI-signed attestation or third-party assurance. Lattica confirms that the source identified below was scanned with lattica-scan (ruleset 104 rules) and that the resulting CycloneDX 1.6 Cryptographic Bill of Materials — whose SHA-256 is recorded below — is a record of the cryptographic assets detected by that scan: 218 findings (14 critical, 41 high, 88 medium).

SUMMARY ID	**SAMPLE-ILLUSTRATIVE-ONLY**
SUBJECT	**acme-payments/api-gateway**
CBOM SHA-256	**9f2c1ea7b4d05583cf0a1d6e84b27c9f3a6e10d8b5147e29c0f8a3b1d2e4c6a70**
CYCLONEDX	**1.6**
RULESET	**104 rules**
SCANNED	**2026-06-15T09:00:00Z**
ISSUED	**2026-06-22T05:31:44.430Z**
VERIFY AT	**https://lattica.dev/cbom/acme-payments/api-gateway**

Supports compliance with

- PCI-DSS 4.0.1 Req 12.3.3 — documented cryptographic cipher/protocol inventory
- FIPS 140-2 to 140-3 transition readiness (Historical List, 21 Sep 2026)
- CNSA 2.0 software/firmware procurement readiness (from 1 Jan 2027)
- NIST FIPS 203 / 204 / 205 migration mapping (ML-KEM / ML-DSA / SLH-DSA)

Reliance & scope: this is a self-issued, point-in-time inventory summary, not a PKI-signed attestation or third-party assurance. It covers a source-and-configuration cryptographic inventory produced by automated rule-based scanning. It does not certify runtime, HSM, cloud-KMS, container, or binary cryptography, and is not a SOC 2 opinion, a QSA assessment, or legal advice. It is intended as evidence supporting an organization's own cryptographic inventory and PQC-migration program.