CRYPTAGION

POST-QUANTUM SECURITY

DISCOVER • SCORE • GENERATE CBOM • REPORT • MIGRATE

Post-Quantum Cryptography Readiness Assessment

Discovery, risk, and migration roadmap

PREPARED FOR

Sample — pyca/cryptography demo

Generated 2026-06-04

Executive summary

Generated by AI assistant (offline fallback — no API key) from 74 discovered assets and the CRYPTAGION risk model.

41	74	73.0%	19	142
CRYPTO POSTURE SCORE	CRYPTOGRAPHIC ASSETS	QUANTUM-VULNERABLE	CRITICAL FINDINGS	PERSON-MONTHS EFFORT

BOARD BRIEFING

Current posture is **EXPOSED**. The maximum asset risk score is **100/100**, with **54** critical/high finding(s) across **34** impacted file(s).

Executive decision required: confirm ownership, fund Wave 1 remediation, and decide whether the inventory becomes a recurring control.

This assessment inventoried 74 cryptographic assets across the scoped systems. 54 (73%) are exposed to a cryptographically relevant quantum computer (CRQC) and 19 carry a CRITICAL rating under our scoring methodology, driven by a combination of algorithm family (predominantly RSA and ECDSA), key-size headroom, and the confidentiality lifetime of the data they protect.

Under the NIST consensus CRQC projection of 2032, any asset protecting data that must remain confidential for more than seven years is already in a harvest-now-decrypt-later exposure window. Adversaries capable of long-horizon intelligence collection can capture this ciphertext today and decrypt it post-CRQC; the appropriate response is migration to the NIST-standardised post-quantum algorithms — ML-KEM (FIPS 203) for key encapsulation, ML-DSA (FIPS 204) for digital signatures, with SLH-DSA (FIPS 205) as a hash-based backup where conservative security assumptions are required.

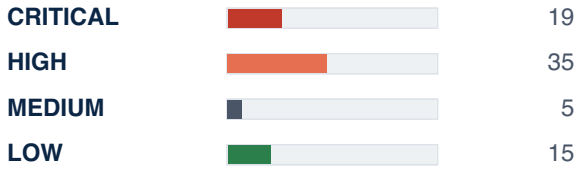
We propose a four-wave migration covering an estimated 142 person-months of effort. Wave 1 (7 assets, 7 pm) targets CRITICAL findings within twelve months and is sized for visible regulator-facing progress. Subsequent waves sequence HIGH and MEDIUM findings against the CRQC projection, with deeply embedded systems deferred to Wave 4. This sequencing is aligned with the obligations CRYPTAGION mapped under: dora, nis2, cra.

Residual uncertainty in CRQC timing should not delay migration of long-lived confidentiality assets. The cost of moving early is bounded; the cost of moving late on already-captured ciphertext is unrecoverable.

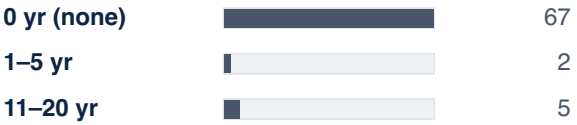
Visual risk dashboard

Board-level view of the risk mix, HNDL exposure, cryptographic family concentration, and migration effort profile.

Risk distribution

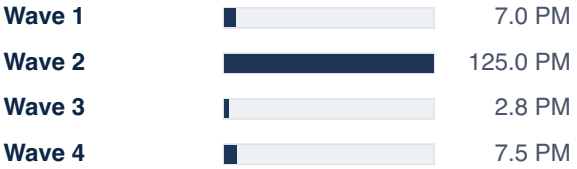


HNDL exposure distribution



Algorithm family concentration

Roadmap effort by wave



30 / 90 / 180 day action plan

WINDOW	FOCUS	RECOMMENDED ACTION	OWNER
0-30 days	Stabilise the evidence baseline	md5 usage	Security architecture + application owners
30-90 days	Remove regulator-visible weak cryptography	Resolve remaining CRITICAL/HIGH findings and document exceptions.	CISO office + engineering leads
90-180 days	Turn the assessment into continuous control	Run recurring scans, publish CBOM deltas, and route remediation into ticketing.	Platform security + GRC

Decisions requested

- Approve ownership for the highest-risk services and certificate estates.
- Fund Wave 1 remediation and exception review within the next quarter.
- Decide whether CRYPTAGION should move from one-shot assessment to continuous monitoring.

Key findings

- 74 cryptographic assets inventoried; 54 quantum-vulnerable.
- 19 CRITICAL findings concentrated in RSA/ECDSA signing and key-wrapping.
- Harvest-now-decrypt-later exposure already material for any asset with a >7-year confidentiality requirement under the NIST 2032 CRQC consensus.
- Wave 1 migration scope sized for regulator-visible delivery within 12 months.
- NIST FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) provide the standardised replacement algorithms across all impacted use cases.

Methodology

> CRYPTAGION inventories cryptographic usage via static analysis of the application source tree and (where applicable) X.509 certificate inventories, cloud KMS APIs, and TLS handshake observation. Each finding is scored against algorithm family, key-size headroom, mode/padding, data sensitivity and confidentiality lifetime, producing a 0–100 quantum-risk score and a category (CRITICAL / HIGH / MEDIUM / LOW). Risk is anchored to the NIST consensus CRQC projection (2032) with optimistic (2030) and conservative (2038) bounds. Replacement algorithms are taken from NIST FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA).

Inventory overview

Breakdown by algorithm family across the scanned scope.

ALGORITHM FAMILY	COUNT
rsa	27
sha2	13
ecdsa	12
aes	7
sha1	6
md5	6
ed25519	3

Risk distribution

CATEGORY	COUNT
CRITICAL	19
HIGH	35
MEDIUM	5
LOW	15

Top 20 highest-risk assets

SCORE	CATEGORY	FAMILY	KEY/ CURVE	MODE/ PADDING	FILE	LINE	REPLACE WITH	BY
100	CRITICAL	md5	—	—	sha1_hasher.py	13	sha2	2027
100	CRITICAL	rsa	—	—	key_manager.py	2	ml-dsa	2027
100	CRITICAL	rsa	4096	—	key_manager.py	9	ml-dsa	2027
100	CRITICAL	rsa	—	OAEP	key_manager.py	19	ml-dsa	2027
98	CRITICAL	sha1	—	—	sha1_hasher.py	7	sha2	2027
92	CRITICAL	rsa	—	PKCS1v15	jwt.py	16	ml-dsa	2027
86	CRITICAL	ecdsa	SECP256R1	—	server.py	7	ml-dsa	2027
86	CRITICAL	ecdsa	—	—	server.py	7	ml-dsa	2027
86	CRITICAL	ecdsa	SECP384R1	—	server.py	12	ml-dsa	2027
86	CRITICAL	ecdsa	—	—	server.py	12	ml-dsa	2027
86	CRITICAL	rsa	—	—	jwt.py	2	ml-dsa	2027
86	CRITICAL	rsa	2048	—	jwt.py	10	ml-dsa	2027
85	CRITICAL	rsa	2048	—	expired_extranet.pem	—	ml-dsa	2027
81	CRITICAL	md5	—	—	hash.js	9	sha2	2027
81	CRITICAL	md5	—	—	LegacyHasher.java	14	sha2	2027
81	CRITICAL	md5	—	—	hash.go	14	sha2	2027
81	CRITICAL	md5	—	—	legacy_hash.c	13	sha2	2027
81	CRITICAL	md5	—	—	legacy_hash.c	19	sha2	2027
76	CRITICAL	rsa	1024	—	iot_device_old.pem	—	ml-dsa	2027
72	HIGH	sha1	—	—	hash.js	5	sha2	2028

Regulatory mapping

DORA Article 9 | NIS2 Article 21 | EU Cyber Resilience Act, Annex I | NIST FIPS 203/204/205

This assessment maps directly to dora, nis2, cra. CRYPTAGION's CycloneDX 1.6 CBOM output is importable into existing GRC tooling and provides the audit trail expected under DORA Article 9 and NIS2 Article 21.

STANDARD / REGULATION	RELEVANCE TO THIS ASSESSMENT
NIST FIPS 203 (ML-KEM)	Replacement for RSA-OAEP, ECDH, and other key-encapsulation use cases.
NIST FIPS 204 (ML-DSA)	Replacement for RSA, ECDSA, Ed25519 digital-signature use cases.
NIST FIPS 205 (SLH-DSA)	Hash-based backup signature scheme for conservative deployments.
EU Cyber Resilience Act	Annex I cryptographic-agility requirements for products entering the EU market.
DORA Article 9	ICT third-party risk and cryptographic resilience obligations for financial entities.
NIS2 Article 21	Cryptographic measures for in-scope essential and important entities.

Migration roadmap

Total estimated effort: **142.2 person-months** across 4 waves.

Wave 1 — Quick wins, regulator-visible

0–6 months · 7 asset(s) · 7.0 PM

ASSET	PRIORITY	EFFORT (PM)
md5 usage	181.25	1.0
sha1 usage	177.62	1.0
MD5 hash usage (broken since 2004)	146.81	1.0
MessageDigest MD5 usage (broken since 2004)	146.81	1.0
md5.New() (broken since 2004)	146.81	1.0
OpenSSL MD5 usage (broken since 2004)	146.81	1.0
OpenSSL MD5 usage (broken since 2004)	146.81	1.0

Wave 2 — High-priority, medium-complexity

6–18 months · 47 asset(s) · 125.0 PM

ASSET	PRIORITY	EFFORT (PM)
SHA-1 hash usage (broken since 2017)	114.84	1.0
MessageDigest SHA-1 usage (broken since 2017)	114.84	1.0
sha1.New() (broken since 2017)	114.84	1.0
OpenSSL SHA-1 usage (broken since 2017)	114.84	1.0
X.509 signature hash: sha1 (intranet.legacy.acme.local)	114.84	1.0
Import of rsa from cryptography.hazmat.primitives.asymmetric	90.62	3.0
RSA key generation (4096-bit)	90.62	3.0
RSA padding: OAEP	90.62	3.0

… and 39 more

Wave 3 — Complex, dependency-heavy

18–36 months · 5 asset(s) · 2.8 PM

ASSET	PRIORITY	EFFORT (PM)
SHA256 usage	113.1	0.25
SHA256 usage	113.1	0.25
X.509 signature hash: sha256 (extranet.acme.legacy.local)	98.6	0.25
AES usage	71.05	1.0
AES mode: GCM	71.05	1.0

Wave 4 — Deeply embedded systems

36+ months · 15 asset(s) · 7.5 PM

ASSET	PRIORITY	EFFORT (PM)
X.509 signature hash: sha256 (internal-ca.acme.eu)	60.9	0.25
SHA256 usage	49.3	0.25
sha256/384/512 New (quantum-safe)	37.7	0.25
sha256/384/512 New (quantum-safe)	37.7	0.25
OpenSSL SHA-2 usage (quantum-safe at SHA-256+)	37.7	0.25
X.509 signature hash: sha256 (client-paris-01)	37.7	0.25
X.509 signature hash: sha384 (vault.acme.internal)	37.7	0.25
X.509 signature hash: sha256 (api.acme.eu)	37.7	0.25
… and 7 more		

Recommended next steps

- Approve the Wave 1 scope and assign a programme owner before the next board cycle.
- Open a cryptographic-agility design review for each Wave 1 service.
- Establish a continuous CBOM refresh process to track migration progress.
- Engage with sectoral regulator early to share the assessment baseline.
- Re-run discovery quarterly to capture new cryptographic usage as it is shipped.

Appendix — data sources

Discovery: Python AST static analysis (extendable to Semgrep for JS/Java/Go/C), X.509 certificate directory scanning, and (Phase 2+) cloud KMS / TLS handshake observation. Risk model: CRYPTAGION's quantum-risk scoring engine, anchored to NIST CRQC consensus (2032) and the algorithm reference in `data/algorithms.yaml`. Export: CycloneDX 1.6 Crypto-BOM, importable into the customer's existing GRC and SIEM tooling.