Post-Quantum Cryptography

Cryptographic Inventory Report

State Health Agency (sample)
System: Patient Records Gateway

Scan date: (reproducible mode — date omitted)
Tool: pqc-check v1.6.0
Scan fingerprint (SHA-256): ca80c71955e102bc813ccb33e9a045a22197599cf28a652db47cf2332cbe84b8

Prepared in alignment with OMB M-23-02 (Migrating to Post-Quantum Cryptography). This report inventories quantum-vulnerable cryptography; it is not an assertion of FIPS 140-3 validation or accreditation.

2. Executive Summary

RED — quantum-vulnerable cryptography in use

Files scanned: 3

Total quantum-vulnerable components: 4

- HIGH (harvest-now-decrypt-later): 3
- MEDIUM: 1
- LOW: 0

Non-vulnerable: not separately enumerated (pqc-check reports only vulnerable usage).

3. Cryptographic Inventory

Algorithm	Param	NIST QSL	Location	Risk
DH Key Exchange	2048	0	src/kex.py:2	HIGH
RSA Key Generation	4096	0	src/keys.js:2	HIGH
DH Key Exchange	—	0	src/keys.js:3	HIGH
ECDSA Signing	—	0	src/sign.go:2	MEDIUM

4. Migration Priority Ranking

Ordered by risk, then harvest-now-decrypt-later exposure (key establishment + encryption before signing).

#	Algorithm	Location	Risk	HNDL
1	DH Key Exchange	src/kex.py:2	HIGH	Yes
2	RSA Key Generation	src/keys.js:2	HIGH	Yes
3	DH Key Exchange	src/keys.js:3	HIGH	Yes
4	ECDSA Signing	src/sign.go:2	MEDIUM	No

5. Recommended Migration Paths

DH Key Exchange
!’ ML-KEM-1024 (FIPS 203)

RSA Key Generation
!’ ML-KEM-1024 (FIPS 203) for key establishment

ECDSA Signing
!’ ML-DSA-87 (FIPS 204)

6. Methodology & Tool Provenance

pqc-check statically scans source code for quantum-vulnerable cryptographic primitives using a compiled-in ruleset (no network access). Detection coverage varies by language and is not a guarantee of quantum-safety.

Tool: pqc-check v1.6.0

CycloneDX CBOM SHA-256: ca80c71955e102bc813ccb33e9a045a22197599cf28a652db47cf2332cbe84b8

Reproducible mode: ON (byte-identical output)

7. Appendix A — Embedded CycloneDX CBOM

The full machine-readable CBOM (CycloneDX 1.6) is reproduced below for verification. Its SHA-256 is recorded in §6.


```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "serialNumber": "urn:uuid:f12c4600-942f-a875-a6a1-c12e63c0d21f",
  "version": 1,
  "metadata": {
    "tools": {
      "components": [
        {
          "type": "application",
          "name": "pqc-check",
          "version": "1.6.0"
        }
      ]
    },
    "component": {
      "type": "application",
      "name": "/tmp/cs-sample2"
    }
  },
  "components": [
    {
      "type": "cryptographic-asset",
      "bom-ref": "PQC-PY-007:src/kex.py:2",
      "name": "DH-2048",
      "cryptoProperties": {
        "assetType": "algorithm",
        "algorithmProperties": {
          "primitive": "key-agree",
          "executionEnvironment": "software-plain-ram",
          "cryptoFunctions": [
            "keygen"
          ],
          "nistQuantumSecurityLevel": 0,
          "parameterSetIdentifier": "2048"
        }
      },
      "evidence": {
        "occurrences": [
          {
            "location": "src/kex.py:2:10"
          }
        ]
      },
      "properties": [
        {
          "name": "pqc-check:patternId",
          "value": "PQC-PY-007"
        },
        {
          "name": "pqc-check:risk",
          "value": "HIGH"
        },
        {
          "name": "pqc-check:category",
          "value": "DH_KEY_EXCHANGE"
        }
      ]
    },
    {
      "type": "cryptographic-asset",
      "bom-ref": "PQC-JS-001:src/keys.js:2",
      "name": "RSA-4096",
      "cryptoProperties": {
        "assetType": "algorithm",
        "algorithmProperties": {
          "primitive": "pke",
          "executionEnvironment": "software-plain-ram",
          "cryptoFunctions": [
            "keygen"
          ],
          "nistQuantumSecurityLevel": 0,
          "parameterSetIdentifier": "4096"
        }
      },
      "evidence": {
        "occurrences": [
          {
            "location": "src/keys.js:2:31"
          }
        ]
      },
      "properties": [
        {
          "name": "pqc-check:patternId",
          "value": "PQC-JS-001"
        },
        {
          "name": "pqc-check:risk",
          "value": "HIGH"
        },
        {
          "name": "pqc-check:category",
          "value": "RSA_KEY_GENERATION"
        }
      ]
    },
    {
      "type": "cryptographic-asset",
      "bom-ref": "PQC-JS-005:src/keys.js:3",
      "name": "DH",
```

```
      "cryptoProperties": {
        "assetType": "algorithm",
        "algorithmProperties": {
          "primitive": "key-agree",
          "executionEnvironment": "software-plain-ram",
          "cryptoFunctions": [
            "keygen"
          ],
          "nistQuantumSecurityLevel": 0
        }
      },
      "evidence": {
        "occurrences": [
          {
            "location": "src/keys.js:3:21"
          }
        ]
      },
      "properties": [
        {
          "name": "pqc-check:patternId",
          "value": "PQC-JS-005"
        },
        {
          "name": "pqc-check:risk",
          "value": "HIGH"
        },
        {
          "name": "pqc-check:category",
          "value": "DH_KEY_EXCHANGE"
        }
      ]
    },
    {
      "type": "cryptographic-asset",
      "bom-ref": "PQC-GO-004:src/sign.go:2",
      "name": "EC",
      "cryptoProperties": {
        "assetType": "algorithm",
        "algorithmProperties": {
          "primitive": "signature",
          "executionEnvironment": "software-plain-ram",
          "cryptoFunctions": [
            "sign"
          ],
          "nistQuantumSecurityLevel": 0
        }
      },
      "evidence": {
        "occurrences": [
          {
            "location": "src/sign.go:2:15"
          }
        ]
      },
      "properties": [
        {
          "name": "pqc-check:patternId",
          "value": "PQC-GO-004"
        },
        {
          "name": "pqc-check:risk",
          "value": "MEDIUM"
        },
        {
          "name": "pqc-check:category",
          "value": "ECDSA_EDDSA"
        }
      ]
    }
  ]
}
```