# Post-Quantum Cryptography

## Cryptographic Inventory Report

**Department of Examples (sample)**
System: Customer Auth Service

Scan date: (reproducible mode — date omitted)
Tool: pqc-check v1.6.0
Scan fingerprint (SHA-256): fdf9a9e0279837afb4338a640b6a4de9223f0015a72e520f2caceb26d33e1e3b

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: 2

Total quantum-vulnerable components: 3

- HIGH (harvest-now-decrypt-later): 2
- MEDIUM: 1
- LOW: 0

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

## 3. Cryptographic Inventory

| Algorithm | Param | NIST QSL | Location | Risk |
|---|---|---|---|---|
| RSA Key Generation | 2048 | 0 | src/auth.py:4 | HIGH |
| TLS Cipher Suite (RSA/DHE) | — | 0 | src/tls.conf:2 | HIGH |
| ECDSA Signing | — | 0 | src/auth.py:7 | MEDIUM |

# 4. Migration Priority Ranking

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

| # | Algorithm | Location | Risk | HNDL |
|---|---|---|---|---|
| 1 | RSA Key Generation | src/auth.py:4 | HIGH | Yes |
| 2 | TLS Cipher Suite (RSA/DHE) | src/tls.conf:2 | HIGH | Yes |
| 3 | ECDSA Signing | src/auth.py:7 | MEDIUM | No |

## 5. Recommended Migration Paths

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

**TLS Cipher Suite (RSA/DHE)**
!’ PQC-enabled TLS (hybrid X25519+ML-KEM-768 !’ ML-KEM-1024)

**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: fdf9a9e0279837afb4338a640b6a4de9223f0015a72e520f2caceb26d33e1e3b

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:5b8fd2cd-78ab-c162-c7f2-fd171754cc19",
  "version": 1,
  "metadata": {
    "tools": {
      "components": [
        {
          "type": "application",
          "name": "pqc-check",
          "version": "1.6.0"
        }
      ]
    },
    "component": {
      "type": "application",
      "name": "/private/tmp/pqc-sample"
    }
  },
  "components": [
    {
      "type": "cryptographic-asset",
      "bom-ref": "PQC-PY-001:src/auth.py:4",
      "name": "RSA-2048",
      "cryptoProperties": {
        "assetType": "algorithm",
        "algorithmProperties": {
          "primitive": "pke",
          "executionEnvironment": "software-plain-ram",
          "cryptoFunctions": [
            "keygen"
          ],
          "nistQuantumSecurityLevel": 0,
          "parameterSetIdentifier": "2048"
        }
      },
      "evidence": {
        "occurrences": [
          {
            "location": "src/auth.py:4:7"
          }
        ]
      },
      "properties": [
        {
          "name": "pqc-check:patternId",
          "value": "PQC-PY-001"
        },
        {
          "name": "pqc-check:risk",
          "value": "HIGH"
        },
        {
          "name": "pqc-check:category",
          "value": "RSA_KEY_GENERATION"
        }
      ]
    },
    {
      "type": "cryptographic-asset",
      "bom-ref": "PQC-CF-004:src/tls.conf:2",
      "name": "TLS",
      "cryptoProperties": {
        "assetType": "algorithm",
        "algorithmProperties": {
          "primitive": "unknown",
          "executionEnvironment": "software-plain-ram",
          "cryptoFunctions": [
            "other"
          ],
          "nistQuantumSecurityLevel": 0
        }
      },
      "evidence": {
        "occurrences": [
          {
            "location": "src/tls.conf:2:13"
          }
        ]
      },
      "properties": [
        {
          "name": "pqc-check:patternId",
          "value": "PQC-CF-004"
        },
        {
          "name": "pqc-check:risk",
          "value": "HIGH"
        },
        {
          "name": "pqc-check:category",
          "value": "CONFIG_FILE"
        }
      ]
    },
    {
      "type": "cryptographic-asset",
      "bom-ref": "PQC-PY-004:src/auth.py:7",
      "name": "EC",
      "cryptoProperties": {
```

```
        "assetType": "algorithm",
        "algorithmProperties": {
          "primitive": "signature",
          "executionEnvironment": "software-plain-ram",
          "cryptoFunctions": [
            "sign"
          ],
          "nistQuantumSecurityLevel": 0
        }
      },
      "evidence": {
        "occurrences": [
          {
            "location": "src/auth.py:7:6"
          }
        ]
      },
      "properties": [
        {
          "name": "pqc-check:patternId",
          "value": "PQC-PY-004"
        },
        {
          "name": "pqc-check:risk",
          "value": "MEDIUM"
        },
        {
          "name": "pqc-check:category",
          "value": "ECDSA_EDDSA"
        }
      ]
    }
  ]
}
```