ODRE PQC v0.2.0

Technical Whitepaper

Application-Embedded Post-Quantum Security Boundary

Canonical Cross-Platform Release
Windows Server 2022 AMD64 / Python 3.12
Ubuntu 24.04 LTS AMD64 / Python 3.12

ODRE AI - Korea
September 2026

1. Executive Summary

ODRE PQC v0.2.0 is the canonical cross-platform release of ODRE's application-embedded post-quantum security boundary for FastAPI. The release was independently verified on Windows Server 2022 AMD64 and Ubuntu 24.04 LTS AMD64, both with Python 3.12.

The public integration contract remains intentionally small:

```
from odre_pqc import install
install(app)
```

The v0.2.0 release uses a common Python wheel across both verified platforms. The cryptographic core and wire protocol were not changed during this cross-platform promotion; the protocol identifier remains **odre-pqc/3**.

FINAL VERDICT: ODRE_PQC_v0.2.0_CROSS_PLATFORM_READY

2. Canonical Release Properties

Property	v0.2.0 result
Product version	0.2.0
Common wheel	PASS
Public install API	install(app)
Cryptographic core changed	NO
Wire protocol changed	NO - odre-pqc/3
Windows runtime / Doctor / Verify / Status / Real PQC	PASS
Ubuntu runtime / Doctor / Verify / Status / Real PQC	PASS
Production changed	NO

3. Security Boundary Model

ODRE PQC is designed to enforce security before protected business logic executes. The security decision is part of the application request path rather than an optional transport decoration.

3.1 Selective Fail-Closed

Protected routes under **/secure/*** are expected to remain closed when the required PQC provider, key, session, integrity, or sequence state is not valid. Public routes remain isolated under the host application's policy.

3.2 Strict Sequence Enforcement

Replay, rollback, gaps, and sequence mismatches are rejected before protected handlers are entered.

3.3 No Silent Classical Downgrade

The verified v0.2.0 evidence reports **AUTO_CLASSIC_DOWNGRADE: 0**. ODRE PQC does not silently substitute classical-only protection for a failed PQC state on protected routes.

3.4 Handler Boundary

The verified results report **HANDLER_BYPASS_WINDOWS: 0** and **HANDLER_BYPASS_UBUNTU: 0** within the defined verification scope.

4. Cryptographic Building Blocks

The public architecture identifies **ML-KEM-768** as the post-quantum key-establishment primitive and **ML-DSA-65** as the post-quantum digital-signature primitive. v0.2.0 did not alter the cryptographic core while promoting the runtime to verified Windows/Ubuntu parity.

5. Cross-Platform Verification Evidence

Verification gate	Windows	Ubuntu
Runtime	PASS	PASS
Doctor	PASS	PASS
Verify	PASS	PASS
Status	PASS	PASS
Real PQC	PASS	PASS
Security regression	61/61 development; 60/60 clean-room	60/60 clean-room
Handler bypass	0	0
Automatic classical downgrade	0	0

Platform parity was separately verified at **20/20 PASS**. No new Critical, High, or Medium findings were reported during the v0.2.0 cross-platform verification.

Verification is scoped evidence. These results do not claim that every possible vulnerability, future attack method, or operational failure has been eliminated.

6. Officially Supported Environments

VERIFIED

Windows Server 2022 AMD64 / Python 3.12
Ubuntu 24.04 LTS AMD64 / Python 3.12

NOT_VERIFIED

Ubuntu 22.04, Debian 12, other Linux distributions, and ARM64 are outside the verified v0.2.0 support matrix.

7. Operator Experience

Doctor diagnoses runtime prerequisites and security configuration. **Verify** exercises real PQC operations and protected-session behavior. **Status** provides read-only visibility into the running protection state. Both official platforms passed all three operational tools as well as Real PQC execution.

8. Platform Verification Inputs

The Ubuntu verification environment used the official Ubuntu 24.04 cloud image and OpenSSL 3.5.8 source as stated in the release evidence. The purpose of these inputs was to establish a reproducible Ubuntu verification environment for the canonical v0.2.0 release.

9. Integrity and Release Artifacts

Artifact	SHA-256
v0.2.0 wheel	`5A9241B8116FEF30B7B408E8805758965FE8825AD30F0DFCBBA625FAC424B120`
Product manifest	`BD9240687467B1AB415F1E1202EEBDF37BF2B029074D4CABE9BF3DA1F2FECF3E`
Windows runtime bundle	`319AAC44372456F9A33C72E686B87F1A9940661B0447C648EEFC47E84DE3FEFB`
Ubuntu runtime bundle	`E149A0ADC7B5527FAC2F273CA2E7A640466614F1A2070BC26338B9DF897B9692`

The preserved v0.1.4 product remains a separate historical baseline. v0.2.0 is the canonical product after successful cross-platform promotion.

10. Production Isolation

The v0.2.0 verification did not modify the production server. The reported production state preserved the existing cng4 process, listeners on 80/443/8000/18081, Nginx, and production code hashes. Health and readiness checks remained HTTP 200. The test Ubuntu VM was shut down after verification.

PRODUCTION_CHANGED: NO

11. Integration Example

```
from fastapi import FastAPI
from odre_pqc import install

app = FastAPI()
install(app)

# /secure/* -> PQC REQUIRED + FAIL-CLOSED
```

12. Release Position

ODRE PQC v0.2.0 is the first canonical release in this product line with independent verification on both officially supported operating environments while retaining a common wheel, the same install(app) public API, the same cryptographic core, and the same odre-pqc/3 wire protocol.

13. Disclaimer

Security verification is scoped evidence, not a guarantee of absolute security. Support claims in this document apply only to the exact environments identified as VERIFIED. Environments marked NOT_VERIFIED must not be represented as verified v0.2.0 platforms.