EchoPulse Golden Test Vector (A5)

Version: 1.0

Date: May 11, 2025

Author: EchoPulse Initiative

This document provides a single, deterministic golden test vector for the EchoPulse Key Encapsulation Mechanism (KEM). This vector can be used to validate the correctness of EchoPulse implementations across different platforms and languages, ensuring consistent behavior in the key derivation process.

1. Vector ID

GTV-001

2. Secret Key (SK)

`7DF3481C90A2B5E637F1D824A9C0E35768B2D41903C5A7E8F21694B0D7E3A5C1`

3. Payload (r)

`AB9102CDEF34567890123456789ABCDEF0123456789ABCDEF0123456789ABCD`

4. v_priv (resolved)

`0x1203`

5. v_enc (resolved)

`0x22FA`

6. Hash Input

`22FAAB9102CDEF3456789O123456789ABCDEF0123456789ABCDEF0123456789ABCD`

7. Derived Key K (SHA3-256)

`8E3B9A2C1D4F6E8A0B2C4D6E8A0B2C4D6E8A0B2C4D6E8A0B2C4D6E8A0B2C4D6E`

8. Purpose

This golden test vector serves as a reproducible and canonical test case for verifying the correctness of the EchoPulse key derivation process, specifically the path from the secret key (SK) through the application of the payload (r) to the final derived shared key (K). Implementations should use this vector to confirm that their symbolic path resolution and SHA3-256 hashing produce the expected intermediate states (v_priv, v_enc) and the final shared key. This vector is suitable for integration into continuous integration (CI) pipelines and regression testing suites to ensure ongoing compliance with the EchoPulse specification.