DCNETWORK

CRYPTOGRAPHIC SOVEREIGNTY

# Post-Quantum Architecture Brief

A crypto-agile backend, architected for post-quantum from day one — against harvest-now-decrypt-later attacks.

For: CISOs & security architects · July 2026 · EU-sovereign, member-owned infrastructure

Attackers are harvesting encrypted data today to decrypt once quantum computers arrive. Most companies are doing nothing. DCNetwork's security stack was architected for post-quantum from day one.

## The threat: harvest now, decrypt later

A sufficiently capable quantum computer breaks the public-key cryptography protecting encrypted email, database backups, and API traffic. Data exfiltrated and stored today becomes readable the day that capability lands — so the migration has to happen before, not after.

## A crypto-agile backend

Encryption sits behind a backend abstraction, so cryptographic primitives can be swapped without re-architecting the application. That is what makes DCNetwork ready to activate NIST-finalized PQC without re-encrypting everything under time pressure.

## The roadmap

Lattice-based encryption — a Kyber-class key-encapsulation mechanism plus Dilithium-class signatures — rolls out behind the existing backend abstraction. Old ciphertexts stay readable through their original backend during the migration window, so nothing breaks mid-transition.

## What this means for you

- No forced re-encryption event — primitives are swapped behind the abstraction.
- Defense against harvest-now-decrypt-later while competitors wait for quantum supremacy to panic.
- Runs on EU-sovereign infrastructure with no dependency on foreign-controlled server fleets.

TALK TO A HUMAN

## De-risk the migration with our team

Request the technical specs, threat model, and implementation roadmap.

Email security@dcnetwork.io · Launch the platform at ai.dcnetwork.io