Q-VAULT

Post-Quantum Hardware Security System

منظومة الأمان السيبراني المتقدمة لما بعد الكم

3 Projects	ML-KEM-768	Zero-Knowledge
Integrated System	NIST FIPS 203	Architecture

Version 1.0 · May 2026 · Q-Vault Development Team

1.— System Overview

Q-Vault هو نظام أمني متكامل يحول شريحة ESP32-S3 إلى مفتاح فيزيائي (Hardware Key) مشفر بخوارزمية ML-KEM-768 المعتمدة من NIST فهو يفتح ويقفل أقراص BitLocker تلقائياً بضمان Zero-Knowledge و Zero-Trust كاملين.

المشاريع الثلاثة — Three Integrated Projects

Project	Language / Stack	Purpose
Q-Vault Service (Windows)	C — Visual Studio 2022	خدمة ويندوز تكتشف USB وتفتح BitLocker
Q-Vault ESP Firmware	C — PlatformIO / ESP-IDF	Firmware ESP32-S3: تخزين Credentials و PQC Handshake
PQC-Vault GUI	C# WPF / .NET	واجهة Provisioning لاختيار القرص وبرمجة ESP32

2.— Technical Architecture

ESP32 Firmware — File Map

File	Lines	Function
src/main.c	287	Entry point — UART init, Setup Mode, Vault Mode, Factory Reset
src/crypto_handshake.c	70	Kyber-768 encapsulation + AES-256-GCM encryption
src/nvs_vault.c	69	NVS read/write/erase for GUID and password
components/kyber/	—	PQClean ML-KEM-768 standalone implementation

Windows Service — File Map

File	Lines	Function
main_service.c	171	Windows Service entry, USB event handler, unlock/lock orchestration
serial_comm.c	209	Full Kyber-768 handshake over COM port
crypto_utils.c	131	BCrypt: AES-256-GCM, SHA-256, HMAC-SHA256, nonce gen
hardware_manager.c	46	COM port discovery via SetupAPI (VID/PID matching)

© 2026 Q-Vault Development Team

File	Lines	Function
vault_bitlocker.c	115	BitLocker unlock/lock via PowerShell stdin pipe

3.— Kyber Handshake Protocol

كل عملية فتح تستخدم Ephemeral Keypair جديد تماماً. يضمن أن كلمة المرور لا تُرسل أبداً بشكل واضح (Plaintext) عبر الـ USB. الـ Handshake

Sequence — تسلسل العمليات

```
Windows Service                          ESP32-S3
──────────────────────────────────────────────────────
   ─── HELLO (5 bytes) ──────────────────────────────▶
   ◀── READY (5 bytes) ──────────────────────────────
   ─── SYNC(0xAABBCCDD) + Kyber PubKey (1184B) ──▶
                                  crypto_kem_enc()
                                  AES-256-GCM encrypt
   ◀── SYNC(0xDDCCBBAA) + Ciphertext (1088B)
         + IV (12B) + Tag (16B) + EncPayload (256B) ──
   crypto_kem_dec() → Shared Secret
   AES-256-GCM decrypt → GUID + Password
   Unlock-BitLocker via PowerShell stdin pipe ✔
```

المعاملات التشفيرية — Cryptographic Parameters

Parameter	Value
KEM Algorithm	ML-KEM-768 (NIST FIPS 203)
Public Key Size	1184 bytes
Secret Key Size	2400 bytes
Ciphertext Size	1088 bytes
Shared Secret	32 bytes
Symmetric Cipher	AES-256-GCM
IV Size	12 bytes (random — esp_fill_random)
Tag Size	16 bytes
Payload	256 bytes (128B GUID + 128B Password)

4.— Security Architecture

نموذج التهديد — Threat Model

Threat Vector	Mitigation
USB Sniffing / MITM	ML-KEM-768 — fresh Ephemeral keypair per session
Quantum Computing Attack	Post-Quantum KEM (NIST FIPS 203 standardized)
Stolen ESP32 (no laptop)	Useless without the paired Windows Service
Stolen Laptop (no ESP32)	BitLocker remains locked — no key stored anywhere
RAM Dumping	SecureZeroMemory() + mbedtls_platform_zeroize()
Password on Command Line	Piped via stdin to PowerShell — never in process args
Remote Factory Reset	Requires physical BOOT button press (5 seconds)

مبادئ الأمان — Core Security Principles

1. Zero-Knowledge Architecture

لأجزاء من RAM ولا ملفات — يتم فيه حفظ كلمة السر. كلمة المرور تعيش في الـ Registry لا يوجد أي مكان على الكمبيوتر — لا الثانية فقط ثم تُعدم برمجياً.

2. Physical Ownership Verification

لمدة 5 ثوانٍ — لا يمكن تفعيلها برمجياً من أي BOOT تتطلب ضغطاً فيزيائياً على زر (Factory Reset) إعادة ضبط المصنع برنامج.

3. Post-Quantum Resistant

لا يمكن كسرها حتى — NIST المعتمدة من ML-KEM-768 بجهاز خارجي، البيانات مشفرة بـ USB حتى لو تم التنصت على منفذ الـ بحاسوب كمي.

5.— System States & LED Codes

LED Status Codes

LED Pattern	Meaning
Solid ON	Setup Mode — awaiting provisioning
5 fast blinks (50ms)	Handshake success / Setup success
3 medium blinks (300ms)	Handshake crypto error
2 long blinks (800ms)	SYNC mismatch or incomplete data

© 2026 Q-Vault Development Team

LED Pattern	Meaning
Rapid toggle while holding BOOT	Factory reset countdown in progress
3 very fast blinks (80ms)	Factory reset confirmed and executed

دورة التشغيل — Daily Usage Workflow

- المستخدم يُدخل ESP32 في منفذ USB
- Windows Service تلتقط إشارة DBT_DEVICEARRIVAL
- الخدمة ترسل HELLO → ESP32 يرد بـ READY
- تُرسل 1184 بايت (Kyber Public Key)
- ESP32 يشفر بيانات القرص ويرسل 1376 بايت
- الخدمة تفك التشفير وتفتح BitLocker عبر PowerShell stdin
- يظهر القرص للمستخدم كـ Drive عادي ✔

- عند سحب ESP32: الخدمة تلتقط DBT_DEVICEREMOVECOMPLETE
- 🔒 على كل البيانات الحساسة SecureZeroMemory + فوراً BitLocker تُقفل

6.— Setup Guide

الخطوة 1: Flash ESP32 Firmware

```
1. Open Q-Vault-ESP in PlatformIO
2. Build → Upload
3. Open Serial Monitor (115200 baud)
4. LED should be SOLID ON (Setup Mode ready)
```

الخطوة 2: Provisioning عبر GUI

```
1. Open PQC-Vault GUI (Run as Administrator)
2. Insert ESP32 → Status shows 'Active on COMx'
3. Select target BitLocker drive from dropdown
4. Choose: Manual password OR Auto-Generate (32-char crypto)
5. Click 'Provision' → GUI sends SETUP command
6. ESP32 blinks 5x and restarts into Vault Mode ✔
```

الخطوة 3: Install Windows Service

```
sc create QVault binPath= "C:\path\to\QVault.exe" start= auto
sc start QVault
```

7.— Future Roadmap

Mobile Companion App (BLE)

- Kill Switch: إغلاق عن بُعد فوري في حالة الطوارئ
- Safe Zone: فتح القرص فقط في شبكات Wi-Fi محددة (BSSID Fingerprinting)
- 2FA عبر Bluetooth مع الـ ESP32

VeraCrypt Integration

- Plausible Deniability — Hidden Volumes داخل الخزنة العادية
- Cascaded Encryption: AES-256 + Twofish + Serpent فوق بعض
- Cross-Platform: دعم Linux و macOS

تحسينات مخططة — Planned Improvements

Feature	Priority	Status
TPM Attestation	High	☐ Planned
Encrypted NVS (eFuse-based)	High	☐ Planned
SafeZone BSSID Fingerprinting	Medium	⚠ Disabled (WLAN cache issue)
Multi-drive support	Medium	☐ Planned
Windows Event Log integration	Low	☐ Planned

Q-VAULT — Protecting your data, one handshake at a time.

تم إعداد هذا المستند في مايو 2026. جميع التفاصيل التقنية مُختبَرة ومُوثَّقة