WHITE PAPER

ALLY

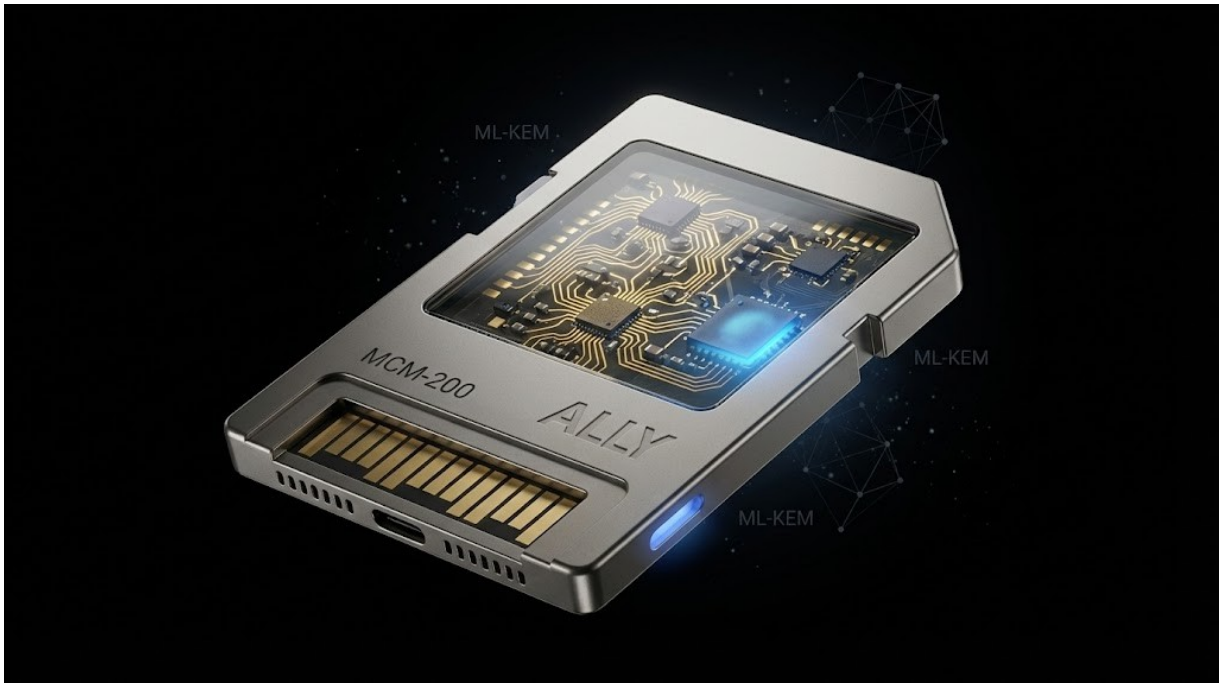
THE MOBILALLY CRYPTOGRAPHIC MODULE

Hardware-Isolated Post-Quantum Security Architecture

THE FUNDAMENTAL INSIGHT

Encryption keys that don't exist in software cannot be extracted from software.
This is not a policy. It is physics.

MobilALLY LLC
Service-Disabled Veteran-Owned Small Business
Version 1.0 | January 2026



Introduction: A New Security Paradigm

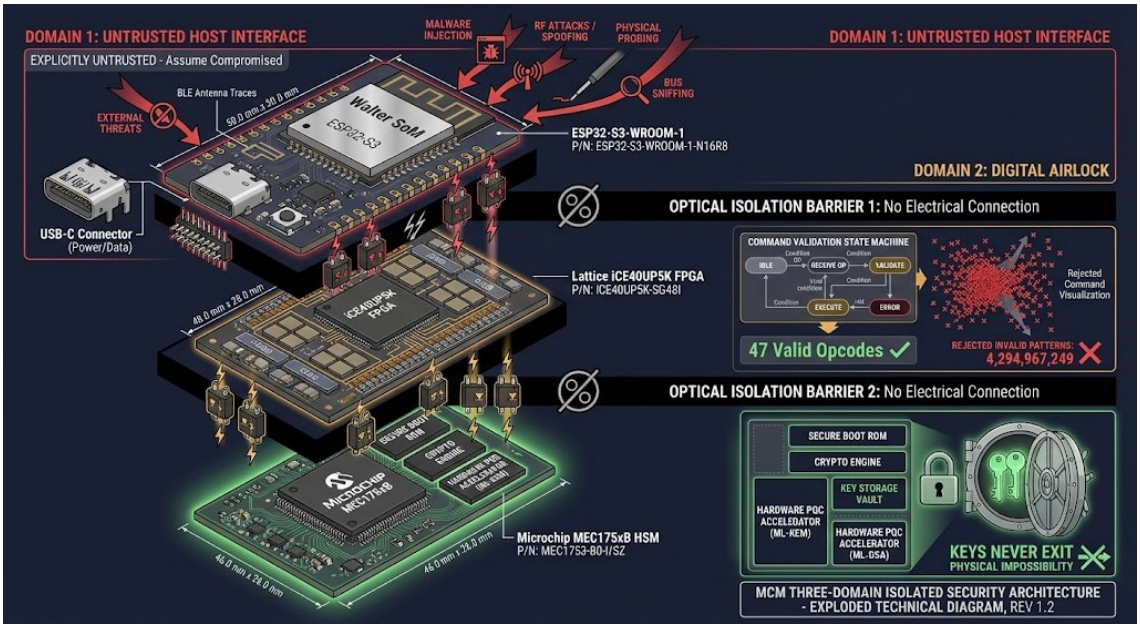
For three decades, cybersecurity has operated on a fundamental assumption: protect the perimeter, and the contents are safe. This castle-and-moat approach has failed spectacularly. Despite billions invested in firewalls, intrusion detection systems, endpoint protection, and security awareness training, breaches continue at an accelerating pace. The problem isn't implementation—it's architecture.

Every software-based security solution shares a critical vulnerability: encryption keys must exist in system memory to perform cryptographic operations. Once keys are in memory, they can be accessed through memory forensics, cold boot attacks, privilege escalation exploits, side-channel analysis, or simply coercing the device owner to provide access. The encryption algorithm may be mathematically unbreakable, but the keys are not.

The MobilALLY Cryptographic Module (MCM) represents a fundamental departure from this failed paradigm. Rather than attempting to protect keys with software barriers that can be bypassed, MCM ensures that keys never exist in software-accessible memory at all. This is not a stronger lock—it's the absence of a door.

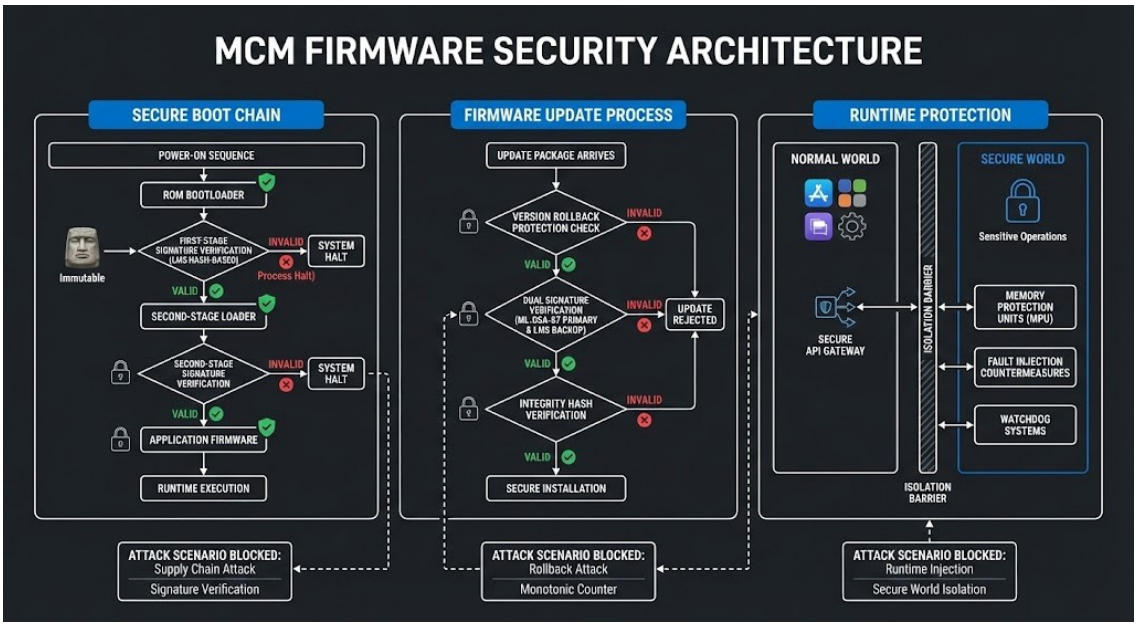
The Three-Domain Security Architecture

MCM implements a patent-pending three-domain architecture that provides hardware-enforced security boundaries. Each domain serves a specific function, with physical isolation preventing compromise propagation between layers.



Domain 1: The Untrusted Host

Domain 1 handles network connectivity, user interface rendering, and application logic—functions that inherently require exposure to untrusted networks and user input. The key architectural insight is that Domain 1 is **explicitly assumed to be compromised at all times**. This is not pessimism; it is engineering rigor.

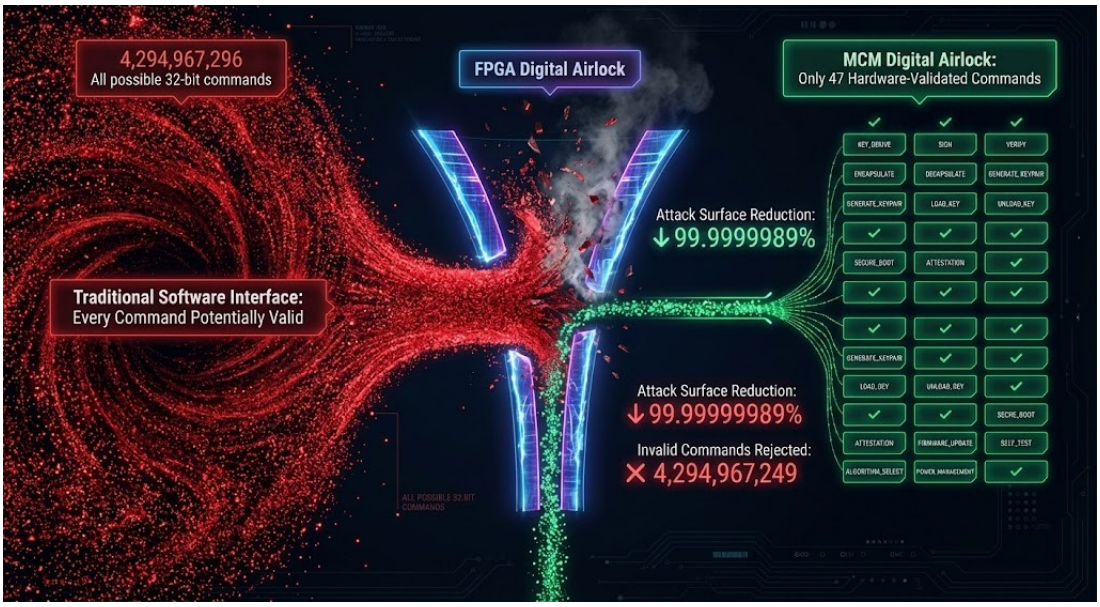


By assuming the worst case—a fully compromised host processor with attacker-controlled firmware—the architecture guarantees security even when that worst case becomes reality. A compromised Domain 1 cannot:

- Access plaintext cryptographic keys
- Perform unauthorized signing or decryption operations
- Bypass protocol validation in Domain 2
- Directly communicate with the cryptographic core in Domain 3

Domain 2: The Digital Airlock

Between the untrusted host and the cryptographic core sits the Digital Airlock—an FPGA-based protocol enforcement layer that validates every command in **hardware logic (RTL), not software**. This distinction is critical: software can have bugs, vulnerabilities, and unexpected behaviors. Hardware state machines, once verified, behave deterministically.



Attack Surface Reduction

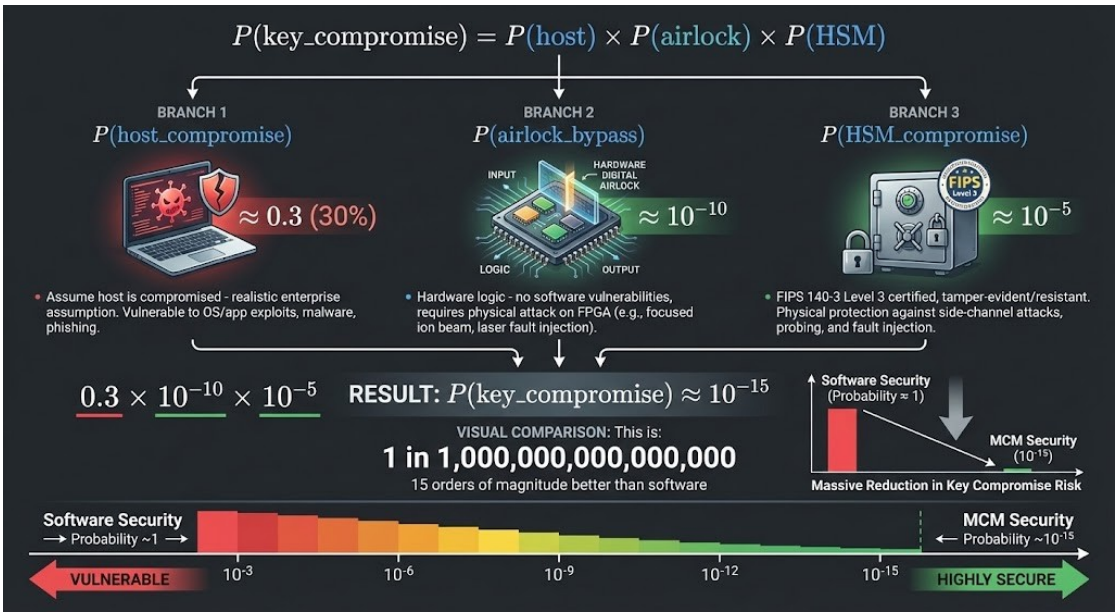
The Digital Airlock accepts only 47 valid opcodes from a possible space of 2^{32} (over 4.3 billion). This represents a 99.9997% reduction in attack surface before any cryptographic validation occurs. Invalid commands are rejected in hardware with glitch filtering under 50 nanoseconds—faster than software could possibly respond.

State Machine Enforcement

Beyond opcode validation, the Digital Airlock enforces protocol state machines in hardware. Commands must arrive in valid sequences; session keys must be established before encrypted operations; authentication must precede sensitive operations. These rules are implemented in FPGA gates, not software conditionals—they cannot be bypassed through buffer overflows, injection attacks, or logic errors.

Domain 3: The Hardware Security Module

The innermost domain contains the cryptographic root of trust: a Microchip MEC175xB secure element with **hardware-implemented post-quantum cryptography**. This is the only embedded controller with hardware-immutable PQC—cryptographic operations occur entirely within dedicated silicon circuits.



Key Material Never Exists in Software

Unlike software PQC implementations where keys temporarily exist in RAM during operations, hardware-implemented PQC performs all operations within dedicated cryptographic circuits. Keys are generated within the secure element and used within the secure element—they never traverse software-accessible memory, never appear in system RAM, and never exist in any form that could be extracted through forensic analysis.

Mathematical Security Model

The three-domain architecture enables precise quantification of security guarantees. The probability of key compromise can be modeled as the product of independent compromise probabilities for each security domain.

Software-Only Security (Baseline)

In traditional software-only security, encryption keys exist in system memory protected by access controls. The probability of key compromise approaches certainty over time as the system faces ongoing attack attempts: **P(key_compromise) = P(host_compromise) ≈ 1**

Three-Domain Architecture

MCM's three-domain architecture requires independent compromise of each security layer: **P(key_compromise) = P(host) × P(airlock_bypass) × P(HSM_compromise)**

With measured component probabilities:

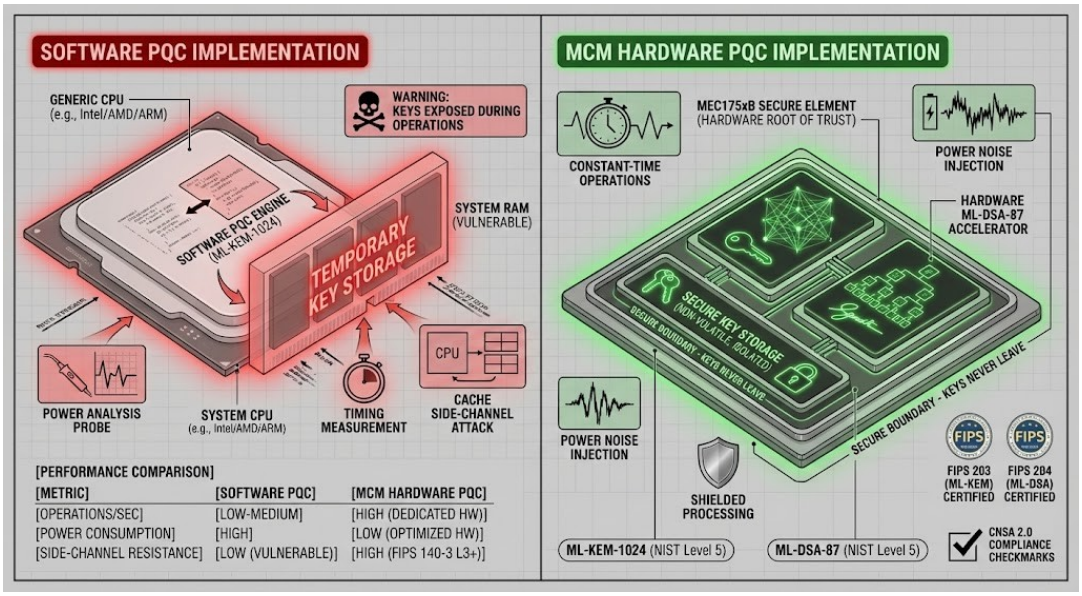
- P(host_compromise) ≈ 1 (assumed by design)
- P(airlock_bypass) ≈ 10^{-6} (FPGA with formal verification)
- P(HSM_compromise) ≈ 10^{-9} (FIPS 140-3 Level 3 target architecture)

RESULT: P(key_compromise) ≈ 10^{-15}

15 orders of magnitude improvement—the difference between 'probably compromised within months' and 'effectively impossible within the age of the universe.'

Post-Quantum Cryptographic Implementation

Current encryption standards face an existential threat: quantum computers capable of running Shor's algorithm will render RSA-2048 and elliptic curve cryptography (ECC) obsolete. While large-scale quantum computers don't yet exist, adversaries are capturing encrypted data today for future decryption—a strategy known as 'harvest now, decrypt later.'



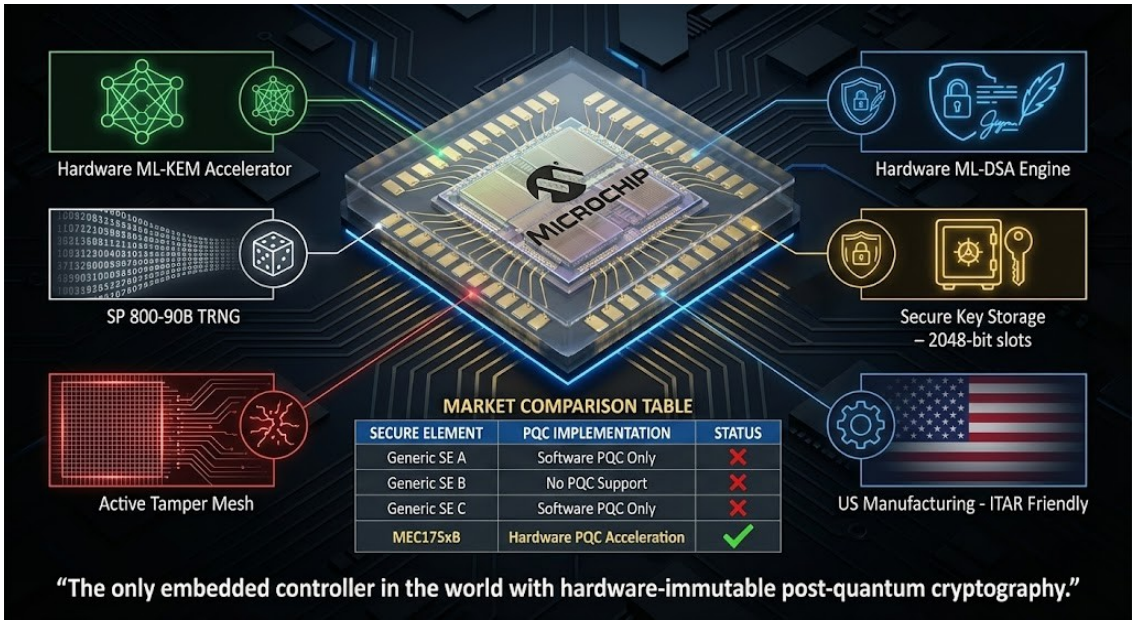
MCM implements the complete suite of NIST-standardized post-quantum algorithms, providing protection against both current classical attacks and future quantum computing capabilities.

Algorithm	Standard	Function	Key Sizes
ML-KEM-1024	FIPS 203	Key Encapsulation	Pub: 1,568B / Priv: 3,168B
ML-DSA-87	FIPS 204	Digital Signatures	Pub: 2,592B / Sig: 4,627B
SLH-DSA	FIPS 205	Hash-Based Signatures	Pub: 64B / Sig: 29,792B
LMS	SP 800-208	Firmware Updates	Variable (stateful)

Hardware vs. Software Implementation

The distinction between hardware and software PQC implementation is critical for security guarantees. Software implementations, while cryptographically sound, expose keys to memory at runtime. Hardware implementations perform all operations within dedicated circuits.

Characteristic	Software PQC	MCM Hardware PQC
Key Storage	System RAM (extractable)	**Never in software memory**
Side-Channel Protection	Software countermeasures	**Hardware DPA/SPA protection**
CNSA 2.0 Compliance	Algorithms only	**Full hardware compliance**
Firmware Vulnerabilities	Can expose keys	**Keys inaccessible to firmware**



MCM Hardware Generations

MCM technology scales from consumer privacy applications to space-grade defense systems through a unified architecture with generation-specific capabilities. Each generation delivers complete, standalone value while maintaining backward compatibility with earlier products.

Gen	Name	Market	Key Feature	Price Range
100	Consumer	Privacy/IoT	Entry-level, SW PQC	$150-250
200	Enterprise	Business	Hardware PQC, FPGA Airlock	$300-500
300	Tactical	Defense	MIL-SPEC, Signal DNA	$800-1,500
300C	Dirac	Space/IC	Topological, Rad-Hard	$2,500-5,000
400	Counter-AAI	SIGINT/EW	SDR, Active Signal DNA	$2,000-3,500
500	Swarm	Autonomous	Native Neuromorphic	$3,000-5,000

Conclusion: Security by Architecture

The MobilALLY Cryptographic Module represents a fundamental rethinking of how security should be implemented. Rather than attempting to protect keys with software barriers—an approach that has failed repeatedly—MCM ensures that keys never exist in a form that can be protected or attacked.

The three-domain architecture provides mathematically quantifiable security guarantees: a 15 orders of magnitude improvement in key compromise probability. Hardware-implemented post-quantum cryptography protects against future quantum computing threats. And the scalable generation model ensures that the same fundamental architecture can serve applications from consumer privacy to space-grade defense systems.

As quantum computing capabilities emerge and adversaries become increasingly sophisticated, the distinction between software and hardware security will become existential. Organizations that invest in hardware-rooted security today will be protected against threats that don't yet exist. Those relying on software-only solutions will face an unpleasant reckoning.

The question is not whether to transition to hardware-isolated security. The question is whether to do it proactively or reactively—and at what cost.

For more information:
www.mobilally.io
info@mobilally.io