DEMO

First chapter only

Quantum-Safe Cryptography for AI Commerce

ML-DSA-65 + Classical Hybrid Signatures in Practice

pragma.vision

TRUSTAUTHORITY.AI

Quantum-Safe Cryptography for AI Commerce

No Affiliation

This book is an independent publication. It is not authorized, sponsored, or endorsed by any of the companies or organizations whose products or services are mentioned herein.

No Professional Advice

The information in this book is provided for educational purposes only. It does not constitute legal, financial, investment, tax, or other professional advice. Readers should consult qualified professionals for guidance specific to their situation.

Code Examples

Code examples in this book are provided for illustration only. They may not be suitable for production use without additional validation, error handling, and security review.

Published by Pragma Vision LLC

First edition, 2026.

Contents

1 The Quantum Threat to AI Commerce 6

1.1 About Pragma.Vision 7

1.2 Why AI Commerce Is Uniquely Vulnerable 8

1.3 The Scale of the Problem 9

1.4 What This Book Covers 9

2 Harvest Now, Decrypt Later: Why Agent Credentials Are at Risk 11

2.1 The HNDL Attack Model 12

2.2 Why Agent Credentials Are Prime HNDL Targets 13

2.3 The Timeline Problem 14

2.4 The Asymmetric Risk Calculation 15

2.5 Signatures vs. Encryption: A Critical Distinction 15

3 NIST Post-Quantum Standards: ML-DSA-65, ML-KEM, SLH-DSA 17

3.1 The Standardization Journey 17

3.2 ML-DSA: The Signature Standard 18

3.2.1 Parameter Sets 18

3.2.2 Why ML-DSA-65 19

3.2.3 Size Comparison 19

3.3 ML-KEM: The Key Exchange Standard 20

3.4 SLH-DSA: The Conservative Backup 20

3.5 What About Falcon? 21

4 The Hybrid Approach: Classical + Quantum-Safe 22

4.1 Why Both, Not Either 23

4.2 External Protocol Constraints . . . 24
4.3 The Hybrid Signature Structure . . . 25
4.4 Verification Logic . . . 25
4.5 Performance Impact . . . 27
4.6 The Three-Layer Protocol Model . . . 27

5 Implementing ML-DSA-65 Signatures . . . 29
5.1 Library Selection . . . 30
5.2 Key Generation . . . 30
5.3 Signing . . . 32
5.3.1 Canonicalization . . . 33
5.4 Verification . . . 33
5.5 Putting It Together: A Complete Signing Service . . . 34
5.6 Testing ML-DSA-65 Implementations . . . 36

6 Hybrid Verification: ECDSA + ML-DSA-65 for AP2, HMAC + ML-DSA-65 for ACP 37
6.1 Protocol-Specific Hybrid Patterns . . . 37
6.1.1 The CryptoService Architecture . . . 37
6.2 AP2: ECDSA + ML-DSA-65 . . . 39
6.2.1 AP2 Mandate Signing . . . 39
6.2.2 AP2 Mandate Verification . . . 40
6.3 ACP: HMAC + ML-DSA-65 . . . 41
6.3.1 ACP Webhook Verification . . . 41
6.4 Database Storage for Hybrid Signatures . . . 43
6.5 Protocol Comparison Summary . . . 44

7 Migration Strategy: From Classical-Only to Hybrid . . . 45
7.1 The Migration Spectrum . . . 46
7.2 Greenfield: The Ideal Path . . . 47
7.3 Brownfield: Phased Migration . . . 47
7.3.1 Phase 1: Inventory and Assessment (Weeks 1–4) . . . 47
7.3.2 Phase 2: Dual-Issue (Months 1–3) . . . 48

7.3.3 Phase 3: Mandatory Hybrid (Months 3–6) . . . 48
7.3.4 Phase 4: Classical Sunset (Months 6–12) . . . 48
7.4 Backward Compatibility Strategies . . . 49
7.4.1 Signature Versioning . . . 49
7.4.2 Feature Flags for Gradual Rollout . . . 50
7.5 Handling the Size Increase . . . 51

8 Future-Proofing: Crypto Agility and Algorithm Upgrades . . . 52
8.1 Why Crypto Agility Matters . . . 53
8.2 Algorithm-Agnostic Design . . . 54
8.3 The Post-Quantum Cryptography Maturity Model . . . 55
8.4 Credential Rotation and Key Lifecycle . . . 56
8.5 Monitoring and Alerting . . . 57
8.6 The Quantum-Maximum Tier . . . 57
8.7 Regulatory Timeline . . . 58
8.8 Summary: The Quantum-Safe Checklist . . . 59

What's Next . . . 61

About Pragma.Vision . . . 63

1

The Quantum Threat to AI Commerce

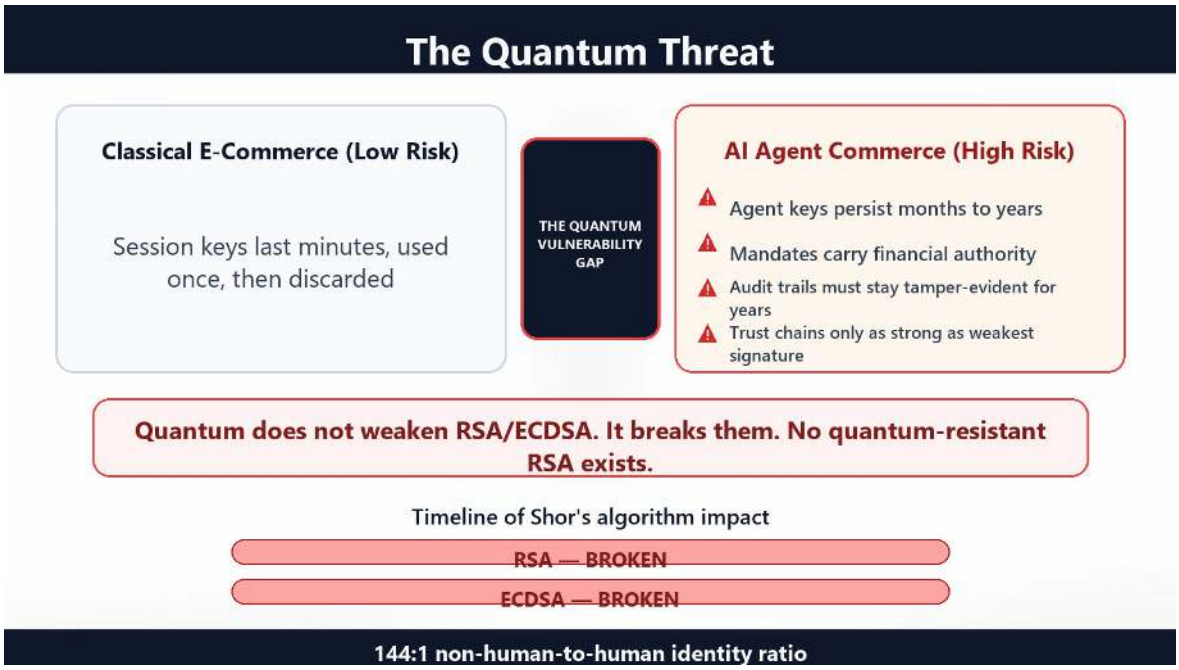

Figure 1. A risk comparison contrasts classical e-commerce, whose session keys last minutes, with AI-agent commerce, whose keys persist months to years and carry financial authority—so Shor's algorithm breaks RSA and ECDSA outright, with no quantum-resistant RSA available

1.1 About Pragma.Vision

Pragma.Vision is an AI-native commerce ecosystem—a growing family of interconnected platforms sharing infrastructure, identity, and payment systems. When an AI agent on wish.now processes a purchase, or a developer on phantoid.com deploys a verified agent, or trust.authority issues a credential, every operation is secured by cryptographic signatures.

Those signatures are the foundation. If the cryptography fails, everything built on top of it fails with it.

This book exists because the cryptography that secures nearly all digital commerce today—RSA, ECDSA, HMAC—faces an existential threat. Not in some distant future.

The threat is active *right now*, even before a single cryptographically relevant quantum computer exists.

1.2 Why AI Commerce Is Uniquely Vulnerable

Classical e-commerce involves a human clicking a "Buy" button and a payment processor charging a credit card. The cryptographic exchange is ephemeral—session keys last minutes, transaction signatures are verified immediately and discarded.

AI commerce is fundamentally different:

- **Agent credentials persist for months or years.** A TrustBadge credential issued to an AI agent today must remain verifiable for the lifetime of that agent—potentially a decade or more.
- **Mandates carry financial authorization.** An AP2 intent mandate cryptographically authorizes an agent to spend up to a specified amount on behalf of a user. If the mandate signature is forged, real money moves.
- **Audit trails must be tamper-evident indefinitely.** Regulatory compliance (SOC 2, GDPR, PCI DSS) demands that transaction logs remain verifiable for years.
- **Agent-to-agent trust chains are only as strong as their weakest signature.** In a multi-agent orchestration—interpretation, matching, negotiation, fulfillment—every link in the chain depends on cryptographic verification.

39%

Probability that quantum computers break RSA-2048 before 2030 (market consensus)[1]

[1]Metaculus community forecast and quantum computing industry estimates, 2025.

1.3 The Scale of the Problem

Every second, millions of cryptographic operations secure digital commerce: TLS handshakes, JWT signatures, webhook verifications, credential issuances. Nearly all of them rely on mathematical problems—integer factorization (RSA) and elliptic curve discrete logarithm (ECDSA)—that quantum computers can solve efficiently using Shor's algorithm.

Warning

A sufficiently powerful quantum computer does not merely *weaken* RSA and ECDSA. It *breaks* them entirely. There is no "quantum-resistant RSA-4096." The mathematical foundation collapses regardless of key size.

The question is not *whether* this will happen, but *when*—and whether the data signed with today's algorithms will still matter on that day.

For AI agent credentials that persist for years, the answer is unambiguously yes.

1.4 What This Book Covers

This book is a practitioner's guide to quantum-safe cryptography for AI commerce systems. It is grounded in real implementation experience—the Pragma.Vision ecosystem has adopted hybrid quantum-safe signatures as its baseline across all platforms, not as a future aspiration but as a present-day default.

You will learn:

1. Why "harvest now, decrypt later" makes quantum threats a *current* risk, not a future one (Chapter 2).
2. What NIST's post-quantum standards (ML-DSA-65, ML-KEM, SLH-DSA) actually specify and how they work (Chapter 3).

3. Why the hybrid approach—classical *plus* quantum-safe, not instead of—is the only responsible strategy (Chapter 4).
4. How to implement ML-DSA-65 key generation, signing, and verification in production systems (Chapter 5).
5. How to build hybrid verification for real payment protocols: ECDSA + ML-DSA-65 for AP2, HMAC + ML-DSA-65 for ACP (Chapter 6).
6. How to migrate from classical-only to hybrid without breaking existing integrations (Chapter 7).
7. How to design for crypto agility so your system survives the *next* algorithm transition (Chapter 8).

Key Insight

This is not a theoretical textbook on lattice-based cryptography. It is an implementation guide written by practitioners who have deployed hybrid signatures in a production AI commerce system. Every code sample in this book reflects real architecture.

DEMO

This is a free preview of the full edition.

Get the complete book at:

https://shop.pragma.vision