Implementing Post-Quantum Cryptography

Future-Proofing Enterprise Security, Compliance and Resilience – From PQC to Business Continuity

Contact:

Thomas Bronack, president
bronackt@dcag.com
(917) 673-6992

DCAG
Data Center Assistance Group, LLC

The Quantum Threat to Data Security

- **Quantum computers** will break current encryption standards
- **Data encrypted today** can be stolen and stored for decryption later ("harvest now, decrypt later") by Hackers
- **Only Post Quantum Cryptography** (PQC) can protect your data, but only if you convert to PQC before data is stolen.
- **Protect** your critical infrastructure, financial systems, supply chains, and sensitive data at risk
- **Timeline:** Quantum computers capable of breaking RSA expected within 5-10 years

Quantum Computing Threat

Current encryption methods like RSA and ECC will be vulnerable to quantum algorithms.

Developing a Quantum-Readiness Roadmap

Shor's Algorithm can factor large numbers exponentially faster than classical computers, breaking encryption that secures your data today. Grover's Algorithm can rapidly crunch numbers

CISA Post Quantum Readiness Report

Password Decryption Cracking times: Now vs Post Quantum Computers

Harvest Now, Decrypt Later (HNDL) , is the most important problem faced by companies today.

Time Required to Decrypt a Password using Classical Computers as compared to Quantum Computers				
Password Length	Charset	Classical Time	Quantum (Grover's)	Quantum (Grover's + Shor's)
6	Alphanumeric + Symbols	12.25 minutes	0.00 sec	1.00 seconds
7	Alphanumeric + Symbols	19.40 hours	0.01 sec	1.01 seconds
8	Alphanumeric + Symbols	10.97 weeks	0.08 sec	1.08 seconds
9	Alphanumeric + Symbols	19.97 years	0.79 sec	1.79 seconds
10	Alphanumeric + Symbols	18.97 centuries	7.74 seconds	8.74 seconds
11	Alphanumeric + Symbols	1802.42 centuries	1.26 minutes	2.26 seconds
12	Alphanumeric + Symbols	171229.78 centuries	12.25 minutes	13.25 seconds
13	Alphanumeric + Symbols	16266829.01 centuries	1.99 hours	2.99 seconds
14	Alphanumeric + Symbols	1545348756.29 centuries	19.40 hours	20.40 seconds
15	Alphanumeric + Symbols	146808131847.72 centuries	1.13 weeks	2.13 seconds
16	Alphanumeric + Symbols	13946772525533.18 centuries	10.97 weeks	11.97 seconds
17	Alphanumeric + Symbols	1324943389925651.50 centuries	2.05 years	3.05 seconds
18	Alphanumeric + Symbols	125869622042936880.00 centuries	19.97 years	20.97 seconds
19	Alphanumeric + Symbols	11957614094079006720.00 centuries	1.95 centuries	2.95 seconds
20	Alphanumeric + Symbols	1135973338937505480704.00 centuries	18.97 centuries	19.97 seconds

Grover's and Shor's algorithms are the major tools used to crack passwords. Grover's algorithm is used to crunch passwords through Brute Force, while Shor's algorithm is used to determine prime numbers. Quantum Computers use Entanglement to half the time needed to crack a password.

Decryption time required to crack a 12-character difficult password changes from centuries to minutes.

Encrypted Data can be stolen now and decrypted later by hackers when quantum computers are available, then they have your most important data to ransom you with.

Laws, Regulations, and supportive Algorithms

Adherence to laws and use of recommended FIPS procedures are necessary for successful PQC Migration.

- All Government agencies must inventory encryption usage.
- Prioritize PQC Migration candidates.
- PQC Inventory and PQC Adoption Plans.
- Develop & Implement PQC Migration Plan.
- All new Systems must use PQC.
- Supply chains must use PQC.
- Migration to PQC completed by 2030.
- Government acceptance of PQC only.

The U.S. federal government has issued clear guidance mandating PQC readiness:

- **6 U.S.C. §1526**: Requires all agencies to inventory cryptographic systems.
- **NSM-10 (National Security Memorandum 10)**: Mandates prioritized migration to PQC.
- **OMB Memorandum M-23-02**: Requires cryptographic inventories and PQC adoption plans from all federal agencies.
- **NSA CNSA 2.0 Requirements**: All new National Security Systems must use quantum-safe algorithms by **2025**. **First Goal**
- By **2030**, RSA-2048 and ECC will be deprecated.
- By **2035**, **only post-quantum cryptography** will be allowed in U.S. government systems.

FIPS and NIST Standards governing PQC adoption

Law / Standard	Mandated By	Mandate Date	Problem Addressed	Certification Required	Certification Deadline	Key Parameters
FIPS 203 (Module-Lattice-Based Key-Encapsulation Mechanism Standard)	NIST	Aug-24	Provides quantum-resistant key encapsulation mechanisms to replace vulnerable public-key encryption methods.	Yes	TBD	Based on CRYSTALS-Kyber algorithm; designed for general encryption with small key sizes and high performance.
FIPS 204 (Module-Lattice-Based Digital Signature Algorithm)	NIST	Aug-24	Offers quantum-resistant digital signature schemes to secure digital communications.	Yes	TBD	Based on CRYSTALS-Dilithium algorithm; provides strong security with efficient verification.
FIPS 205 (Stateless Hash-Based Digital Signature Algorithm)	NIST	Aug-24	Provides alternative digital signature schemes resistant to quantum attacks.	Yes	TBD	Based on SPHINCS+ algorithm; stateless and hash-based, offering strong security assurances.
CNSA Suite 2.0 Commercial National Security Algorithm Suite 2.0)	NSA	Sep-22	Updates cryptographic algorithms to be quantum-resistant for national security systems.	Yes	Transition period ongoing	Includes recommendations for using quantum-resistant algorithms; specific algorithms and parameters defined by NSA.
NIST SP 800-208 (Recommendation for Stateful Hash-Based Signature Schemes)	NIST	Oct-20	Provides guidance on using stateful hash-based signature schemes as interim solutions until PQC standards are finalized.	No	N/A	Recommends usage of algorithms like XMSS and LMS for specific applications requiring long-term security.
FIPS 140-3 (Security Requirements for Cryptographic Modules)	NIST	Mar-19	Specifies security requirements for cryptographic modules, including those implementing PQC algorithms.	Yes	Transition period until September 2026	Successor to FIPS 140-2; includes updated requirements to accommodate PQC algorithms.

Understanding the Data Supply Chain

- Data Supply Chain, feeds, and In-house data
- **Vulnerability:** Data creation points may lack encryption standards
- **Solution:** Use PQC to protect when data is received and stored

- Structured and Unstructured Data
- **Vulnerability:** Essential encrypted data can be harvested now, and decrypted later
- **Solution:** Use PQC to protect data at rest. Protection provided by Homomorphic Encryption and Data Centric Security.

- Networks, APIs, and cloud services
- **Vulnerability:** Data in transit encryption often overlooked
- **Solution:** Use PQC to protect data transfer through Homomorphic Encryption and Data Centric Security.

Post-Quantum Cryptography: The Solution

- Mathematical algorithms resistant to quantum computing attacks
- NIST standardization process nearing completion
- Provides protection against both classical and quantum threats
- Enables forward security for sensitive data

Key Benefits of PQC Implementation

Future-proof security: Protection against both classical and quantum attacks

Regulatory compliance: Meet emerging requirements from government and industry

Forward security: Ensure today's sensitive data remains protected tomorrow

Standardized approach: NIST-approved algorithms provide reliability

Regulatory Landscape

Federal Regulations

- **FISMA:** Requiring quantum-resistant solutions for federal systems
- **FedRAMP:** Adding PQC requirements for cloud service providers
- **NIST:** Finalizing standardization of PQC algorithms

Industry Regulations

- **HIPAA:** Implications for healthcare data protection
- **PCI DSS:** Considerations for financial information security
- **SEC:** Potential disclosure requirements for quantum readiness

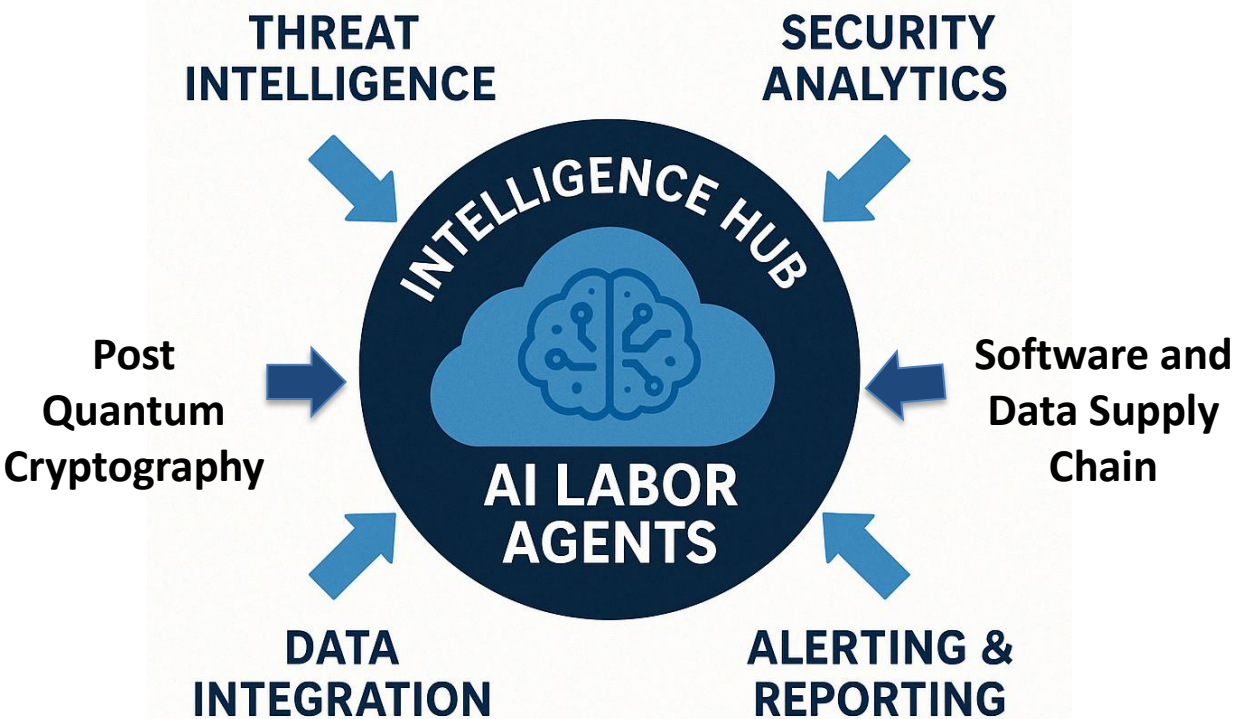
International Frameworks

- **EU:** NIS2 Directive and GDPR implications
- **China:** National standards for quantum-safe cryptography
- **Global:** ISO/IEC standards for cryptographic technique

AI Agentic Rag automation for optimization

AI Agents can be used to automate functions associated with PQC Migration or Maintenance.

AI Agentic RAG



Implementation Strategy

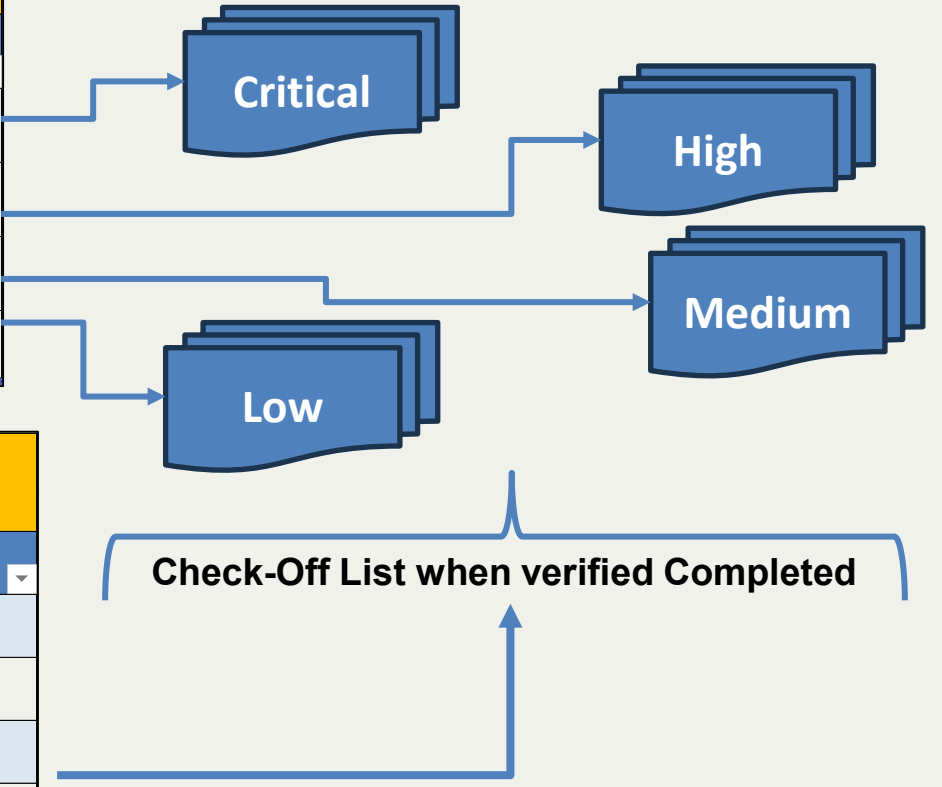
Phase 1	Phase 2	Phase 3	Phase 4	Phase 5
Discovery and Assessment of encryption assets.	Risk analysis and prioritization	Solution selection and testing	Deployment and monitoring	Continuous improvement
• Discovery Phase • Identify all encryption uses • Catalog crypto libraries • Document key lengths	• Evaluate data sensitivity • Assess protection lifetime • Prioritize critical systems • Develop Check-off list	• Choose NIST algorithms • Develop test environments • Measure performance impact	• Implement hybrid solutions • Roll out in priority order • Check completed migrations off list • Monitor for issues	• Perform Regular cryptographic reviews • Follow standards evolution • Provide Continuous Training • Update as needed

Encryption Discovery Report

Results required from Encryption Discovery Report				
Discovery Element	**Description**	**Why It Matters**	**Prioritization Criteria**	**Verification Method**
Cryptographic Algorithm Type	RSA, ECC, DSA, AES, SHA, etc.	Quantum vulnerability	Asymmetric = High	Crypto scan + simulation
Key Length	**1024, 2048, 4096 (RSA); 256-bit (AES)**	**Indicates strength**	**<2048-bit = Critical**	**Key strength checker**
Encryption Purpose	Data-at-rest, data-in-transit, etc.	Scopes urgency	Transit + key exchange = Critical	Protocol mapping
Protocol/Library Used	**TLS 1.2/1.3, OpenSSL, etc.**	**Identifies upgrade paths**	**Legacy = Critical**	**Protocol inspection tools**
Certificate Details	X.509 certs, CA info	Needs PQC-ready PKI	RSA/ECC certs = High	Cert audit tools
Hardware Crypto Modules	**HSMs, TPMs**	**Compatibility or upgrade**	**Fixed crypto = High**	**Device interrogation**
Embedded or Hardcoded Keys	In firmware, binaries	Hard to rotate/upgrade	Static keys = Critical	Binary scanning
Software Components (SBOM)	**Dev/vendor SBOMs**	**Maps crypto dependencies**	**Legacy crypto = High**	**SBOM/CBOM analysis**
Data Sensitivity	PII, PHI, FCI, CUI	Prioritizes replacements	Regulated data = Critical	Data tagging
Usage Context	**APIs, cloud, internal**	**Exposure urgency**	**Public exposed = High**	**Traffic analysis**

Analysis, Prioritization, and Verification of PQC Migration

Prioritizing Phase II Migration Cycles based on Prioritization		
Risk Level	**Criteria**	**Recommended Schedule**
Critical	RSA < 2048-bit, expired certs, public exposure, etc.	Immediate (0–3 months)
High	ECC key exchange, TLS 1.2, vendor apps	Short-term (3–6 months)
Medium	SHA-1, AES-128, internal APIs	Mid-term (6–12 months)
Low	AES-256, TLS 1.3, internal-only	Long-term (12–24 months)



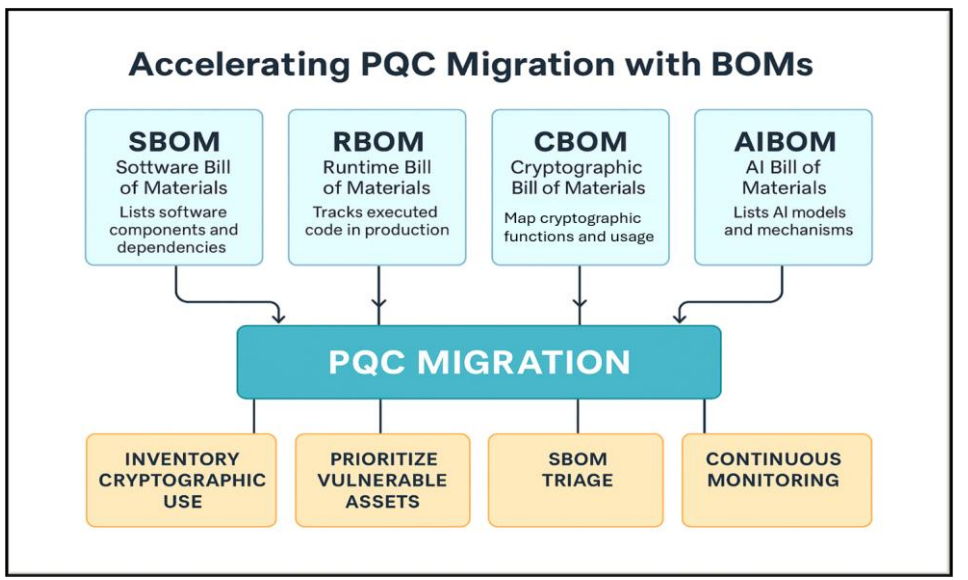
Verification of PQC Migration	
Verification Method	**Purpose**
Simulated Message Exchange	Confirms PQC functional integrity in key exchange/signing
Hybrid Certificate Testing	Tests interoperability of legacy + PQC certs
Compliance Scanners	Ensure conformance with FIPS 203–205, CNSA Suite 2.0
Cryptographic Audit Reports	Documents configuration and PKI compatibility
PKI Compatibility Testing	Validates CA support for PQC certs
Automation Scripts	Verify PQC in CI/CD builds, detect legacy crypto

Technology Comparison

Provider	Solution Type	Key Features	Implementation Ease	Cost Factors
GemaSecure	Specialized PQC solutions for enterprise	Comprehensive ecosystem, legacy integration, managed services	Medium (requires dedicated resources)	Subscription-based, scales with deployment size
Microsoft	PQC integration with existing products	Azure Key Vault integration, Windows/Office support	Easy (for Microsoft environments)	Included in enterprise licensing
Google	Open-source PQC implementations	Boringssl library, Chrome browser support	Complex (requires development expertise)	Free open-source, implementation costs
NVIDIA	Hardware acceleration for PQC algorithms	GPU acceleration, high- performance computing support	Complex (specialized hardware)	Hardware investment plus integration
AWS	Cloud-based PQC services	KMS integration, S3 encryption options	Medium (requires AWS expertise)	Pay-per-use model based on API calls

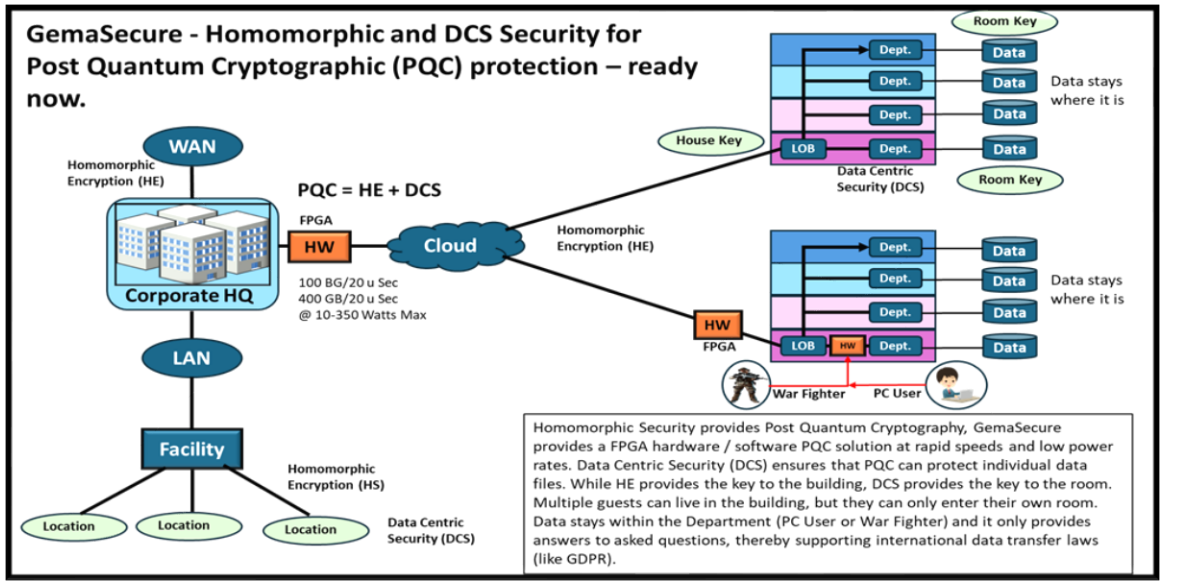
DCAG partner firms in PQC Migration - What ProCap360 and GemaSecure products provide

Discovery, Analysis, Monitoring and Dashboard



ProCap360 provides Bills of Materials (Software, Release Components, Cryptographic usage, and AI) that support obtaining the information needed to perform a Post Quantum Cryptography (PQC) migration. It discovered your current use of encryption, so that you can develop a migration path in waves from critical to least important data needing migration to PQC.

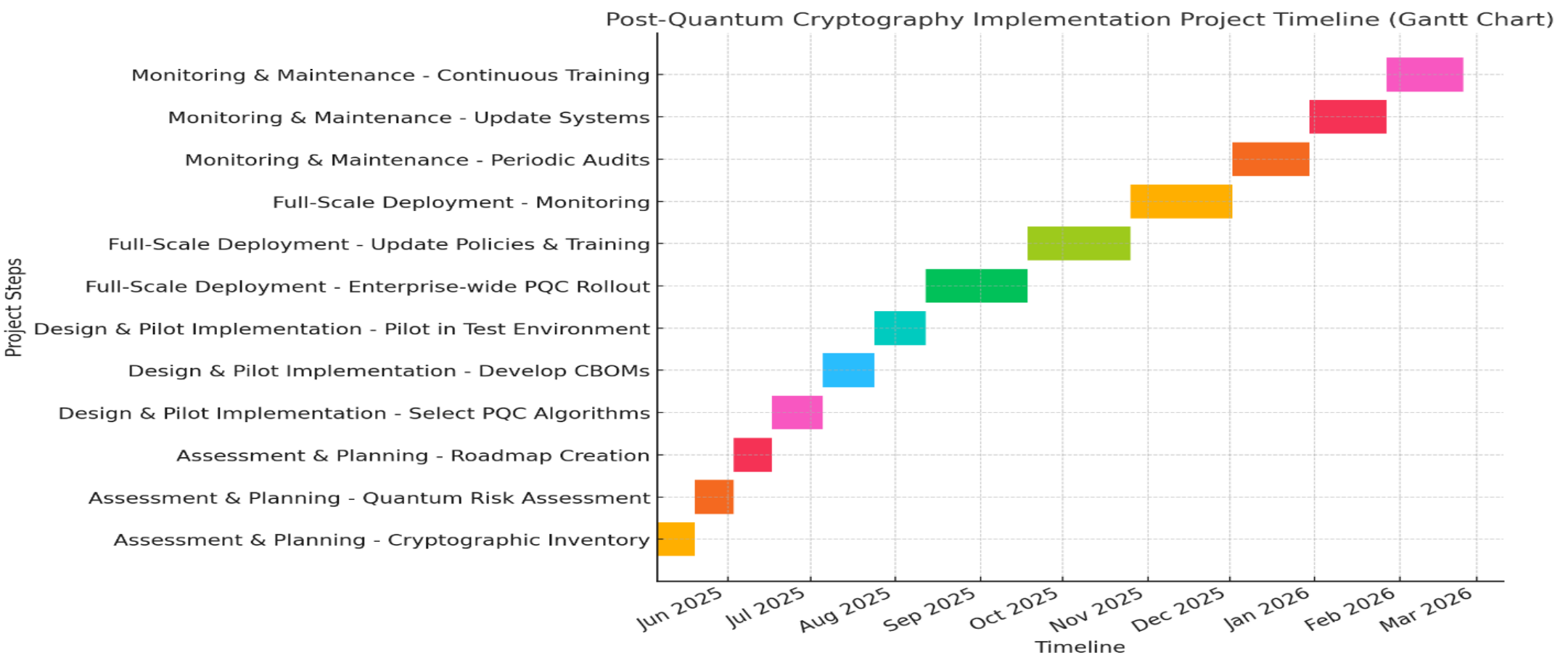
Distributed PQC Hardware / Software Solutions – Ready Now!



GemaSecure provides the hardware and software needed to implement Post Quantum Cryptography today through Field Programmable Gate Arry (FPGA) hardware with optimized software that results in ultra-fast cryptography at greatly reduced power consumption rates. GemaSecure handles structured and non-structured data (i.e., Data Lakes, Data Bases, Videos, Images, Voice, etc.) and provides Homomorphic and Data Centric Security over components.

Project Plan and timeline

Approximately a 2–3-year project to implement PQC in a medium sized company.



Project Personnel Requirements & Skills
Plus, cost estimates for services

Role	Number Needed	Key Skills
Project Manager	1	Project coordination, stakeholder communication, risk management
Cryptography Expert	1–2	Deep understanding of PQC algorithms, cryptographic systems
Security Analyst	2–3	Risk assessment, vulnerability analysis, compliance knowledge
Systems Engineer	2–3	System integration, network architecture, performance tuning
DevSecOps Specialist	1–2	CI/CD pipelines, security automation, infrastructure as code
Training Coordinator	1	Developing training materials, conducting sessions, feedback collection

Phase	Duration	Consulting Hours	Cost (@$150/hr)
Assessment & Planning	4–6 weeks	240–360	$36,000–$54,000
Design & Pilot Implementation	6–8 weeks	360–480	$54,000–$72,000
Full-Scale Deployment	12–16 weeks	720–960	$108,000–$144,000
Monitoring & Maintenance	Ongoing	Varies	Varies
Total	22–30 weeks	1,320–1,800	$198,000–$270,000

Business Case for PQC Implementation

- **Risk mitigation:** Protect against future quantum attacks
- **Competitive advantage:** Early adoption demonstrates security leadership
- **Compliance:** Meet emerging regulatory requirements
- **Customer trust:** Ensure long-term data protection
- **Protect Against Harvest Now, Decrypt Later (HNDL):** Protect your most important encrypted data from being copied now and decrypted later by Hackers. Once they have your data, there is nothing you can do to protect yourself.

ROI Considerations

Implementation costs: $250K-$500K for mid-sized enterprise

Cost of breach: Average $4.45M per incident (IBM 2023)

Risk reduction: Early implementation reduces exposure by 65%

Market advantage: 73% of customers value future-proof security

Next Steps

- **Executive sponsorship** and resource allocation
- Establish **PQC implementation team**
- **Discover** where encryption is presently being used and priority components and data usage
- Develop detailed **technical project plan** with migration waves
- Begin **cryptographic inventory assessment**
- Partner with **DCAG** for implementation support

Timeline

Month 1-2: Assessment and team formation

Month 3-4: Risk analysis and solution selection

Month 5-8: Testing and pilot implementation

Month 9-18: Phased full deployment

Secure Your Data Supply Chain Today

- The **quantum threat** is real and approaching rapidly
- **Present data is exposed** to HNDL attacks by Hackers
- PQC implementation is a strategic necessity
- DCAG provides expert guidance through the entire process

Contact us to begin your quantum-safe journey

DCAG

PQC Advisory Group

Email: bronackt@dcag.com

Phone: (917) 673-6992

Schedule a Consultation

Contact Information

Data Center Assistance Group, LLC

- bronackt@dcag.com
- bronackt@gmail.com
- (917) 673-6992
- www.dcag.com