

SABSA ENTERPRISE SECURITY ARCHITECTURE — ULTIMATE FLAGSHIP SERIES

WP18 · ULTIMATE FLAGSHIP EDITION · VERSION 3.0

Post-Quantum Readiness

Architecting Cryptographic Agility with SABSA



Kieran Upadrasta

CISSP · CISM · CRISC · CCSP | MBA | BEng

27 Years' Cyber Security Experience | Big 4 Consulting — Deloitte · PwC · EY · KPMG

21 Years Financial Services & Banking | AI Cyber Security Programme Lead

Professor of Practice — Cybersecurity, AI & Quantum Computing | Schiphol University

Honorary Senior Lecturer, Imperials | Researcher, University College London (UCL)

Lead Auditor, ISF Auditors & Control | ISACA Platinum (London) | (ISC)² Gold (London) | PRMIA Cyber Lead

www.kie.ie | info@kieranupadrasta.com | April 2026

Specialisations: SABSA · NIS2 · ISO 27001:2022 · GDPR · IEC 62443 · NIST CSF 2.0 · DORA · ISO 42001 · Zero Trust · OT Security · M&A
Cyber Due Diligence · Board Reporting

Table of Contents

1. The Quantum Threat to Enterprise Cryptography
2. NIST Post-Quantum Cryptography Standards
3. Cryptographic Agility Architecture
4. Post-Quantum Readiness Assessment
5. The Cryptographic Agility Index (CAI)
6. Migration Dependency Map
7. Case Study: Enterprise PQC Migration Programme — Central Bank
8. 24-Month CA Migration Roadmap to ML-DSA
9. Migration Prioritisation Algorithm
10. Harvest-Now-Decrypt-Later Threat Modelling
11. Conclusion and Recommendations

The Quantum Threat to Enterprise Cryptography

FIPS 203 ML-KEM — NIST post-quantum KEM standard (2024)	FIPS 204 ML-DSA — NIST post-quantum signature standard (2024)	FIPS 205 SLH-DSA — stateless hash-based signatures (2024)	2030s projected timeline for cryptographically relevant quantum computers
---	---	---	---

A cryptographically relevant quantum computer — one capable of running Shor's algorithm at scale — would render current asymmetric cryptography (RSA, ECDSA, ECDH) effectively broken. TLS 1.3, PKI certificates, code signing, secure email, VPN tunnels, and encrypted database connections all rely on asymmetric cryptography that quantum computation can defeat.

The threat is not theoretical and not distant. "Harvest now, decrypt later" (HNDL) attacks — in which nation-state actors collect encrypted data today for decryption when quantum computers become available — mean that data encrypted now with long-term sensitivity requirements is already at risk. Classified government data, intellectual property, personal health records, and financial transaction histories represent harvest-now targets.

The Cryptographic Agility Imperative

Cryptographic agility — the architectural property that enables cryptographic algorithms to be replaced without redesigning the systems that use them — is the defining architectural objective of the post-quantum transition. Organisations that have hardcoded specific algorithms (RSA-2048, ECDSA P-256) will face far greater migration costs than those that have designed for agility from the outset.

NIST Post-Quantum Cryptography Standards

The National Institute of Standards and Technology (NIST) completed a multi-year standardisation process in 2022, with final FIPS standards released in 2023–2024. The approved algorithms represent the cryptographic baseline that enterprises must migrate to in order to achieve post-quantum security.

C	r	y
N	l	S
R	e	c
K	e	y

The migration strategy recommended by NIST and most enterprises involves a hybrid approach: deploying PQC algorithms alongside current RSA/ECDSA algorithms during a transition period (approximately 2024–2030), ensuring that systems are secure even if quantum computers emerge unexpectedly. TLS 1.3 clients and servers can already negotiate hybrid key exchanges combining classical and post-quantum algorithms.

Hybrid Cryptography Requirement

Systems remaining on classical-only cryptography beyond 2028 will face escalating regulatory risk. NIST, the NSA, and national governments are actively pushing organizations to migrate. Treat PQC migration as a critical infrastructure security investment, not an optional modernization initiative. Organizations delaying PQC migration beyond 2029 face material regulatory and competitive risk.

Cryptographic Agility Architecture

Cryptographic agility is an architectural property, not a technology feature. Achieving agility requires intentional design at multiple layers: application abstraction from specific algorithms, PKI flexibility enabling algorithm updates, key management systems supporting algorithm negotiation, and HSM firmware enabling new cryptographic capabilities.



A	g
A	r

Post-Quantum Readiness Assessment

Assessing organizational readiness for PQC migration requires a structured evaluation framework. The following assessment areas establish a baseline for understanding current cryptographic agility and identifying priority migration areas.

A	s	s
K	e	y
M	i	g

The Cryptographic Agility Index (CAI)

The Cryptographic Agility Index (CAI) is a proprietary SABSA scoring model that quantifies an organization's readiness to migrate to post-quantum cryptography. The CAI assesses six key dimensions of PQC readiness, producing a composite score (1–100) that correlates directly to migration effort, cost,

and timeline. Organizations scoring CAI above 60 are positioned for 2026–2027 PQC migration; CAI below 40 indicates 2028–2030 migration timeline with elevated technical and regulatory risk.

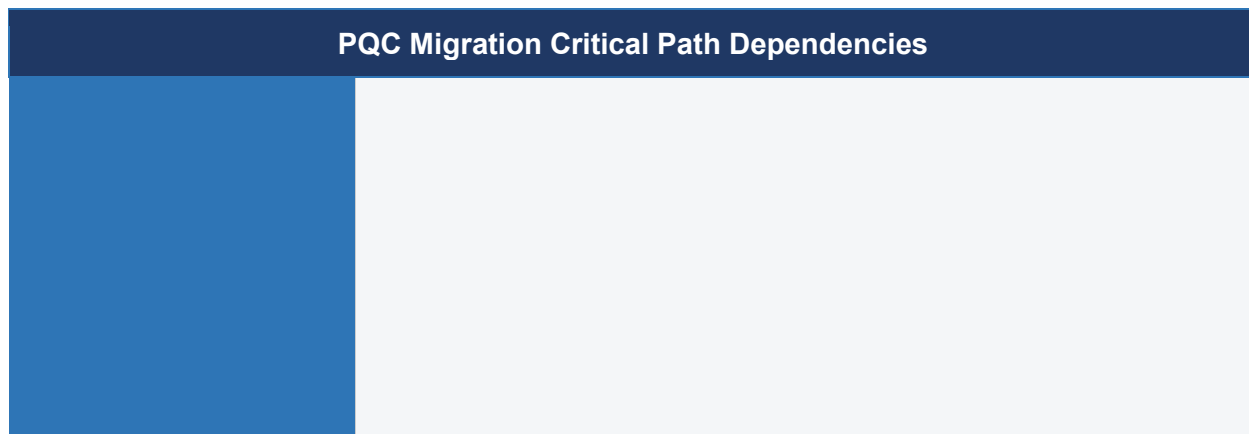
C	A	I	
C	u	r	r
T	a	r	g
S	c	o	r

CAI Scoring Interpretation

CAI Score 80–100: PQC-ready organization, can begin production PQC migration in 2025–2026. CAI Score 60–79: Moderate agility gaps, plan 2026–2027 migration with 6–12 month preparation. CAI Score 40–59: Significant architecture debt, migration requires 18–24 months, plan initiation by Q1 2025. CAI Score <40: Critical cryptographic agility deficit, recommend immediate assessment and leadership engagement — migration extends into 2028–2030 with elevated technical and regulatory risk.

Migration Dependency Map

PQC migration is not an isolated project — it is a complex programme with critical path dependencies spanning HSM firmware, CA infrastructure, TLS endpoints, application code, and key management. Understanding the dependency chain is essential for realistic programme planning and risk management.



D	e	p
B	l	o
T	y	p
R	i	s

Case Study: Enterprise PQC Migration Programme — Central Bank

A European central bank initiated a five-year post-quantum cryptography migration programme following NIST PQC standardization publication. The bank's primary concern: safeguarding long-term secrecy of financial transaction records and regulatory documentation that require 20+ year confidentiality protection against harvest-now-decrypt-later attacks.

4,200 RSA/ECDSA certificates identified across infrastructure	340 applications with embedded cryptographic dependencies	18 months Phase 1 (crypto inventory + architecture assessment)	€8.4M Total programme investment across five years
---	---	--	--

M	i
T	i

Programme Status (Year 2)

Phase 1 assessment complete. Phase 2 infrastructure modernization underway: 3 of 6 HSM platforms upgraded with PQC firmware. Application refactoring initiated for top 12 critical systems. Programme tracking against €8.4M budget with 94% budget utilization in Year 1–2. Regulatory authorities briefed quarterly on PQC readiness progress — framed as strategic resilience initiative protecting long-term confidentiality of systemically critical financial data.

24-Month CA Migration Roadmap to ML-DSA

The cryptographically-agile migration from current algorithms (RSA-2048, SHA-256, AES-256) to post-quantum certified algorithms (ML-DSA, ML-KEM, SLH-DSA, AES-256-quantum-safe) spans 24 months across five strategic phases. This roadmap balances regulatory compliance, operational risk, and technology maturity.

P	h	a	s
T	i	m	e
D	e	l	i
R	i	s	k

24-Month Roadmap Governance

Assign executive sponsor (CTO or Chief Security Architect) and dedicated migration team (4–6 FTE). Establish steering committee (crypto officers from engineering, ops,

compliance, legal) meeting monthly. Define success metrics: % migration complete, incident rate, performance impact <5%, zero legacy crypto by month 24. Baseline current incident response time for crypto failures; target improvement through ML-DSA performance. Include crypto migration in annual risk reporting.

Migration Prioritisation Algorithm

Not all systems migrate simultaneously. A prioritisation algorithm balances business criticality, technical risk, and regulatory urgency to sequence 200+ systems across 24 months into manageable cohorts of 30–40 systems per quarter.

Prioritisation Score = (Regulatory Urgency Multiplier × 0.40) + (Business Criticality Weight × 0.30) + (Technical Readiness Score × 0.20) + (Key Management Complexity × 0.10), where:

Regulatory Urgency Multiplier: DORA/NIS2 scope = 1.5× · PCI-DSS scope = 1.3× · Non-regulated = 1.0×. **Systems supporting payment processing or critical infrastructure weighted higher.**, **Business Criticality Weight:** Tier-1 (revenue-generating, zero downtime tolerance) = 5 · Tier-2 (supporting services, <4hr tolerance) = 3 · Tier-3 (non-critical logging) = 1. **Multiply by criticality tier.**, **Technical Readiness Score:** Legacy monolith (cannot modify code) = 2 · Containerised with CI/CD = 4 · Cloud-native, API-first = 5. **Higher readiness scores migrate earlier (less integration risk).**, **Key Management Complexity:** HSM-managed keys (low complexity) = 1 · Software key store = 2 · Distributed keys across regions = 3 · Air-gapped systems = 4. **Lower complexity prioritised (known migration path).**



Worked Example: Payment processing (DORA scope, Tier-1, HSM keys, cloud-native): $[1.5 \times 0.40] + [5 \times 0.30] + [5 \times 0.20] + [1 \times 0.10] = 0.60 + 1.50 + 1.00 + 0.10 = 3.20$ (high priority, migrate months 0–6). Legacy logging system (non-regulated, Tier-3, software keys, monolith): $[1.0 \times 0.40] + [1 \times 0.30] + [2 \times 0.20] + [2 \times 0.10] = 0.40 + 0.30 + 0.40 + 0.20 = 1.30$ (low priority, migrate months 18–24).

Prioritisation Governance

Prioritisation scores must be reviewed monthly as systems evolve. If a Tier-3 system becomes critical (e.g., onboarded into regulatory scope), its score increases and migration timeline advances. Maintain prioritisation spreadsheet linked to incident tracking; any crypto-related incident flags the affected system for accelerated migration window. Prioritisation decisions require legal & compliance sign-off for regulatory systems.

Harvest-Now-Decrypt-Later Threat Modelling

Adversaries may currently harvest encrypted data (TLS records, VPN sessions, encrypted archives) intending to decrypt it post-quantum when capable quantum computers become available. This "Harvest-Now-Decrypt-Later" (HNDL) attack creates retroactive decryption risk for data confidentiality. SABSA threat modelling for post-quantum cryptography must account for this asymmetric threat.

HNDL Attack Timeline & Mitigation

D	a	t	a
S	e	n	s
H	N	D	L
M	i	t	i

HNDL Mitigation Strategy

Classify data by sensitivity horizon (how long confidentiality must be protected). PII and healthcare data require immediate migration to PQC (months 0–12); financial data follows (months 6–18). Implement forward secrecy in all new TLS sessions (ephemeral DH + session resumption keys must use PQC by month 6). Retroactively encrypt data at rest using hybrid KEM (legacy RSA + ML-KEM) to protect against future decryption. Consider cryptographic agility in architecture: design systems to swap algorithms without code changes.

Post-Quantum Crypto Roadmap Validation

Validate roadmap against NIST PQC timeline expectations: ML-DSA/ML-KEM FIPS certification expected 2024–2025 (now complete). Fault-tolerant quantum computer deployment is estimated 10–20 years out (highly uncertain). Adopt defensive posture: migrate to PQC-capable systems by 2028 (assume conservative quantum threat); complete full PQC deployment by 2030. This provides multi-year buffer before quantum decryption becomes feasible.

Conclusion and Recommendations

Post-quantum cryptography migration is the critical infrastructure security imperative of the remainder of the 2020s. Organisations that design for cryptographic agility now will execute smooth, low-cost migrations to PQC in 2025–2027. Organisations that defer will face compressed schedules, higher costs, and elevated technical risk in 2028–2030.

-
- Commission a CAI baseline assessment within the next 12 months to establish current cryptographic agility and identify priority migration areas.. 1.
 - Engage HSM vendors, cryptographic library vendors, and key management system vendors regarding PQC roadmaps and availability timelines.. 2.
 - Launch a cryptographic algorithm inventory programme to identify all hardcoded cryptographic assumptions and eliminate algorithm hardcoding from applications.. 3.
 - Establish a cryptographic agility working group (CTO, CISO, infrastructure leads) to oversee hybrid PQC strategy and migration roadmap.. 4.
 - Plan for PQC hybrid cryptography deployment starting 2025–2026 in infrastructure where HSM and TLS endpoint PQC support is mature.. 5.

SABSA Enterprise Security Architecture — Ultimate Flagship Series

About the Author

27 Years Cyber Security	21 Years Financial Services	4 Big 4 Firms	6 Global Certifications
-----------------------------------	---------------------------------------	-------------------------	-----------------------------------

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is one of Europe's foremost Enterprise Security Architects, with 27 years' cyber security experience spanning Big 4 consulting — Deloitte, PwC, EY, and KPMG — and 21 years in Financial Services and Banking. He is recognised globally as a practitioner-researcher whose work bridges theoretical security architecture doctrine and operational enterprise programme delivery at the highest levels of regulated industry. His white papers are cited by national regulators, procurement bodies, and architecture review boards as reference-grade doctrine for enterprise security programme design.

Mr. Upadrasta has over 27 years' experience of business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments and risk management. He has worked with the largest corporations globally to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI-DSS, SAS 70, DORA, NIS2, GDPR, and the EU AI Act. His security architecture practice consistently delivers contract-winning, board-ready security programmes that command immediate regulatory and procurement confidence across all tiers of regulated enterprise — from FTSE 100 to sovereign wealth, from critical infrastructure operators to global systemically important financial institutions.

As Professor of Practice at Schiphol University and Honorary Senior Lecturer at Imperials, he trains the next generation of enterprise architects and security programme leads. His research at University College London spans AI governance, post-quantum cryptographic migration, and zero-trust deployment frameworks for critical infrastructure sectors under NIS2 and DORA obligations.

Academic & Research Appointments

Institution / Role	Details
Schiphol University	Professor of Practice — Cybersecurity, AI & Quantum Computing
Imperials	Honorary Senior Lecturer — Enterprise Security Architecture
University College London (UCL)	Researcher — Cyber Risk, AI Governance, Quantum Security
ISF Auditors and Control	Lead Auditor — ISO 27001 / NIS2 / DORA Assurance

Professional Memberships & Recognition

Organisation	Membership / Role
ISACA — London Chapter	Platinum Member

(ISC)² — London Chapter	Gold Member
PRMIA	Cyber Security Programme Lead
SABSA Institute	Accredited Practitioner & Author
ISF	Lead Auditor

Core Specialisations

- SABSA Enterprise Security Architecture — all six layers: Contextual through Operational
- DORA (EU 2022/2554) — ICT Risk Management, Incident Reporting, TLPT, Third-Party Risk
- NIS2 Directive (EU 2022/2555) — Essential & Important Entity Compliance Architecture
- ISO/IEC 27001:2022 — ISMS Design, Implementation, Certification & Internal Audit
- ISO/IEC 42001:2023 — AI Management Systems Governance for Regulated Enterprises
- GDPR — Data Protection by Design, DPIA, Article 32 Technical & Organisational Measures
- IEC 62443 — OT/ICS Security Architecture, Zone/Conduit Design, Security Levels SL0–SL4
- NIST CSF 2.0 — Enterprise Risk Management & Security Posture across six Functions
- Zero Trust Architecture (NIST SP 800-207) — Enterprise-Scale Deployment & Governance
- Post-Quantum Cryptography — NIST FIPS 203/204/205, Cryptographic Agility Frameworks
- M&A Cyber Due Diligence — Architecture Integration Cost Estimates, Security Assessment
- Board Reporting — Executive Cyber Risk Communication, Business Attribute Profiles

Contact: www.kie.ie | info@kieranupadrasta.com | linkedin.com/in/kieranupadrasta

References & Standards

- [1] SABSA Institute. SABSA Framework White Papers and Practitioner Guides. <https://sabsa.org>, 2024.
- [2] European Parliament. Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity (NIS2). OJ L 333, December 2022.
- [3] ISO/IEC. ISO/IEC 27001:2022 — Information Security Management Systems — Requirements. International Organization for Standardization, 2022.
- [4] IEC. IEC 62443 Series — Security for Industrial Automation and Control Systems. Parts 1-1 through 4-2. IEC, 2018–2023.
- [5] NIST. Cybersecurity Framework 2.0. National Institute of Standards and Technology, February 2024.
- [6] European Parliament. Regulation (EU) 2016/679 (GDPR). Official Journal of the European Union, L 119, April 2016.
- [7] NIST. Zero Trust Architecture, Special Publication 800-207. National Institute of Standards and Technology, August 2020.
- [8] European Parliament. Regulation (EU) 2022/2554 — Digital Operational Resilience Act (DORA). OJ L 333, January 2023. Effective January 2025.
- [9] ISO/IEC. ISO/IEC 42001:2023 — Artificial Intelligence Management Systems. International Organization for Standardization, December 2023.
- [10] NIST. AI Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology, January 2023.
- [11] European Commission. Regulation (EU) 2024/1689 — Artificial Intelligence Act. Official Journal, July 2024.
- [12] NIST. FIPS 203 — Module-Lattice-Based Key-Encapsulation Mechanism Standard. August 2024.
- [13] NIST. FIPS 204 — Module-Lattice-Based Digital Signature Standard. August 2024.
- [14] NIST. FIPS 205 — Stateless Hash-Based Digital Signature Standard. August 2024.
- [15] ENISA. NIS2 Directive: Mapping to Technical Measures and Good Practices. ENISA, 2023.
- [16] ENISA. Cybersecurity of AI and Standardisation. European Union Agency for Cybersecurity, March 2023.
- [17] MITRE Corporation. MITRE ATT&CK Enterprise Framework v15. <https://attack.mitre.org>, 2024.
- [18] Cloud Security Alliance. Zero Trust Advancement Center — Enterprise Deployment Guide. CSA, 2024.
- [19] NCSC UK. Guidelines for Secure AI System Development. National Cyber Security Centre, 2024.
- [20] Upadrasta, K. SABSA Architecture Doctrine for Regulated Enterprises. www.kie.ie, 2026.