MICKAI™

MICKAI EBOOK SERIES · PLAYBOOK No. 3

Post-Quantum Audit for Critical National Infrastructure.

An operator-side playbook for the NCSC migration roadmap, the 2031 high-priority infrastructure deadline, and the 2035 universal cryptographically-relevant deadline.

AUTHOR

Micky Irons

Founder and named inventor, Mickai LTD.
Crunchbase · LinkedIn · GitHub · mickai.co.uk

DATE · 14 May 2026 · v1

EBOOK · No. 3 IN A SERIES OF FOURTEEN

Mickai LTD · Companies House 17166618 · press@mickai.co.uk · mickai.co.uk
UK IPO register GB2607309.8 to GB2611702.8 and GB2611885.1 onwards · Trade mark UK00004373277

TABLE OF CONTENTS

Contents

Foreword

A note from the author

Part I · The Deadlines

1. 2031 for high-priority infrastructure
2. 2035 universal cryptographically-relevant
3. What the NCSC actually requires at hour zero

Part II · The Operator-side Migration

4. Inventorying the cryptographically-relevant systems
5. ML-KEM (FIPS 203) and ML-DSA (FIPS 204) explained
6. Hash-linking under the SHA-3 family
7. Hybrid and pure-PQ deployment models

Part III · The Audit-Chain Side

8. Post-quantum signed audit for AI workloads
9. ML-DSA-87 migration path from ML-DSA-65
10. Key custody, rotation, and revocation

Part IV · Engagement

11. NCSC, ICO, OFCOM, OFGEM, OFWAT engagement
12. Procurement clauses for PQC readiness
13. The transferable artefact
14. Closing

Appendix

About the author
References and further reading

FOREWORD

A note from the author

The NCSC has published the post-quantum cryptography migration roadmap. The dates are 2031 for high-priority critical national infrastructure and 2035 for universal migration. The substrate question is what an operator at National Grid, SSE, BT, Openreach, Thames Water, Severn Trent, the major UK banks, or the Nuclear Decommissioning Authority portfolio actually does on Monday morning to land on those dates without a vendor-key dependency.

This ebook is the operator-side playbook. It reads the deadlines, walks the FIPS 203 and FIPS 204 primitives, gives the inventory and sequencing discipline, and shows the engineering counterpart for the AI audit chain surface specifically. The substrate primitive is the Open Audit Record (OAR), which is post-quantum-signed from inception and migrates cleanly across the ML-DSA-65 to ML-DSA-87 parameter set boundary.

The Mickai substrate primitives are filed at the UK Intellectual Property Office across the GB2607309.8 to GB2611702.8 and GB2611885.1 onwards families. The trade mark Mickai is registered at UK00004373277.

Micky Irons

Founder and named inventor, Mickai LTD · 14 May 2026

PART I · THE DEADLINES

What the NCSC migration roadmap requires of CNI operators

1. 2031 for high-priority critical national infrastructure

The NCSC roadmap, published as part of the cross-government cryptographic agility programme, sets 2031 as the date by which UK high-priority critical national infrastructure must complete cryptographic migration to post-quantum primitives. The high-priority designation covers transmission and distribution networks (National Grid, the regional DNOs), water (Thames Water, Severn Trent, United Utilities, the wider water sector), telecoms backbone infrastructure (BT, Openreach, Virgin Media O2), central banking and clearing systems (Bank of England, CHAPS, BACS), and the nuclear estate (NDA portfolio, EDF civil reactors, defence-nuclear primes through MOD assurance routes).

The 2031 date is the operator's date, not the vendor's date. NCSC guidance is explicit that the obligation sits with the system operator, not with the supplier ecosystem. An operator that is, in 2031, still running ECDSA-signed TLS certificates on systems within the high-priority boundary is non-compliant with the roadmap regardless of whether the vendor of the certificate authority has migrated.

2. 2035 universal cryptographically-relevant

The 2035 date is the universal migration deadline. By 2035, every cryptographically-relevant system in the UK regulated estate must run on post-quantum primitives for confidentiality (ML-KEM, FIPS 203), integrity and authentication (ML-DSA, FIPS 204), and hash-based operations (SHA-3 family, FIPS 202). The remaining four-year window between 2031 and 2035 accommodates the long tail (embedded firmware, IoT devices with hard-coded crypto, legacy code-signing infrastructure, and other systems where the migration cost is bounded but the deployment schedule is constrained).

> **The 2035 deadline is the operator's compliance horizon. The substrate primitive should sit on PQC from inception, not migrate to it at the horizon.**

3. What the NCSC actually requires at hour zero

At hour zero of a regulator engagement, the NCSC asks four questions of a CNI operator. First, what is the inventory of cryptographically-relevant systems? Second, what is the migration plan against the 2031 and 2035 deadlines? Third, what evidence chain demonstrates that the migration is being executed against the plan? Fourth, where the system is dependent on a third-party vendor's PQC readiness, what is the contractual position that holds the vendor to the same deadlines?

The operator that has answers to all four questions is on the roadmap. The operator that has answers only to the first two is exposed. The operator that has no inventory is, in 2026, the typical case; the rest of this ebook is the playbook for moving out of that position.

PART II · THE OPERATOR-SIDE MIGRATION

Inventory, sequence, migrate

4. Inventorying the cryptographically-relevant systems

The first step is inventory. Every system in the CNI operator's estate that uses cryptography must be enumerated, categorised by the primitive in use, and ranked by upgrade complexity. The inventory is system-by-system, primitive-by-primitive, with an explicit owner per row.

Surface	Typical primitive (today)	Target (2031/2035)
TLS termination on web frontends	ECDHE + ECDSA + SHA-256	ML-KEM + ML-DSA + SHA-3
Code signing for firmware and software	RSA-2048 or ECDSA	ML-DSA-65 or ML-DSA-87
Document signing for regulated artefacts	RSA-2048 or ECDSA	ML-DSA-65
VPN tunnels (site-to-site, remote access)	ECDHE + AES-GCM	ML-KEM + AES-GCM
IoT firmware integrity at edge devices	ECDSA on hardware root	ML-DSA-65 on hardware root
AI audit trail signing	ECDSA or RSA (when signed at all)	ML-DSA-65 (OAR substrate)
Database column encryption	AES-256-GCM with classical KEM wrap	AES-256-GCM with ML-KEM wrap
Hash linking for tamper-evident logs	SHA-256	SHA-3-512

5. ML-KEM (FIPS 203) and ML-DSA (FIPS 204) explained

ML-KEM (FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism, finalised August 2024) is the post-quantum key exchange primitive that replaces classical Diffie-Hellman variants (ECDHE, RSA-KEM). ML-KEM-768 ships approximately 192 bits of classical security and 128 bits of post-quantum security; ML-KEM-1024 ships 256 and 192 respectively. The 1024 parameter set is recommended for systems whose confidentiality must hold against a cryptographically-relevant quantum attacker for decades after the data is captured.

ML-DSA (FIPS 204, Module-Lattice-Based Digital Signature Algorithm, finalised August 2024) is the post-quantum digital signature primitive that replaces classical signatures (ECDSA, RSA-PSS). ML-DSA-65 ships approximately 192 bits of classical security and 128 bits of post-quantum security; ML-DSA-87 ships 256 and 192. The Mickai OAR substrate uses ML-DSA-65 by default with an upgrade path to ML-DSA-87 at the operator's discretion.

6. Hash-linking under the SHA-3 family

SHA-3-512 (FIPS 202, Keccak family) is the hash function the Mickai substrate uses for hash-linking the OAR audit chain. SHA-3 is not, by itself, a post-quantum migration target; SHA-256 and SHA-512 remain secure against a quantum attacker (Grover's algorithm only quadratically speeds up hash preimage search, so the SHA-2 family retains adequate margin). The selection of SHA-3 in the Mickai substrate is for portability with the CBOR canonical encoding profile, not for quantum resistance.

7. Hybrid and pure-PQ deployment models

Two deployment models coexist during the migration window. Hybrid mode runs a classical primitive (ECDH or ECDSA) and a post-quantum primitive (ML-KEM or ML-DSA) in parallel; the combined output is secure as long as either is. Hybrid is the default for TLS migration (the IETF is standardising hybrid-PQ TLS variants). Pure-PQ mode runs only the post-quantum primitive and is the default for new deployments where downgrade risk to a non-PQ peer is bounded.

The Mickai OAR substrate runs pure ML-DSA-65 by default; the audit chain is intended to verify decades after capture, so hybrid offers no additional safety property and adds verifier complexity. Other surfaces (TLS in particular) typically run hybrid during the migration window.

PART III · THE AUDIT-CHAIN SIDE

The AI audit surface specifically

8. Post-quantum signed audit for AI workloads

AI audit trails are typically signed using classical primitives (ECDSA or RSA-PSS) by AI vendors who do not control their own PQC roadmap. A regulator in 2031 walking a four-year-old AI audit trail signed under ECDSA-P256 faces a chain that is no longer cryptographically-relevant under NCSC guidance. The operator that lands AI audit signing on ML-DSA-65 today is ahead of the deadline by construction.

The OAR substrate documented in Ebook #2 of this series is post-quantum-signed from inception. Every record in the chain is signed under ML-DSA-65, hash-linked under SHA-3-512, and replayable through the browser-resident verifier at any point in the lifetime of the chain. The migration question for an AI workload at a CNI operator reduces, in this surface, to wrapping the vendor's decision-emit hook with the OAR primitive and routing the signed records to the operator's chain store.

9. ML-DSA-87 migration path from ML-DSA-65

The ML-DSA-87 parameter set provides 256 bits of classical and 192 bits of post-quantum security, against ML-DSA-65's 192 and 128. ML-DSA-87 is the conservative parameter for systems whose audit chain must hold against a stronger future quantum attacker, or where the system operator is constrained to the highest available NIST security level for regulatory or contractual reasons.

The Mickai OAR substrate supports the ML-DSA-65 to ML-DSA-87 upgrade through the standard key rotation path. The operator schedules a rotation, the SIOS issues a chain anchoring record under the active ML-DSA-65 key that binds a new ML-DSA-87 public key to the chain identifier, and subsequent records are signed under the new key. The chain continues to verify across the rotation boundary; the verifier walks both signature schemes.

10. Key custody, rotation, and revocation

Key custody at a CNI operator is hardware-rooted. The ML-DSA private key lives in the operator's hardware security module (HSM) or in TPM 2.0 bound to the workstation's platform configuration registers. The key never leaves the hardware; signing is delegated and the signature is emitted back to the SIOS for inclusion in the OAR record.

Rotation is policy-driven. The default Mickai rotation policy is annual, with a thirty-day overlap window during which both keys are valid. Revocation is explicit; the operator issues a revocation record under the new active key declaring the prior key revoked from a stated timestamp. Records signed before the revocation timestamp remain VERIFIED; records signed after become REVOKED in verifier output.

PART IV · ENGAGEMENT

From inventory to regulator-engaged migration

11. NCSC, ICO, OFCOM, OFGEM, OFWAT engagement

The migration sits inside a multi-regulator engagement model. The NCSC owns the cross-government roadmap. The ICO covers UK GDPR-relevant cryptographic posture across data subjects. OFCOM covers telecoms; OFGEM covers energy; OFWAT covers water; the PRA covers banking; the ONR covers nuclear; the MHRA covers pharma. Each sector regulator has, in 2026, an engineering desk that can receive a thirty-minute substrate briefing under the existing engagement framework.

The recommended engagement sequence is: brief the NCSC engineering contact first, brief the relevant sector regulator second, and use the joint position to drive the procurement clauses in section 12.

12. Procurement clauses for PQC readiness

Every AI vendor procurement, every cryptographic service procurement, every HSM and TPM procurement, and every code-signing certificate procurement issued in 2026 and forward should carry post-quantum readiness clauses. The Mickai recommended baseline clause set is:

· The supplier shall demonstrate a documented PQC migration plan against the NCSC 2031 and 2035 deadlines.
· All cryptographic primitives in the supplied system shall be agile, with the migration path from classical to ML-KEM / ML-DSA / SHA-3 explicitly versioned.
· The supplier shall, at no additional cost, replace any non-compliant primitive prior to the 2031 deadline for the high-priority surface and prior to the 2035 deadline for the universal surface.
· The operator retains the right to verify any cryptographic evidence chain produced by the system using independent, open-source, browser-resident verifier tooling without reliance on the supplier's infrastructure.
· The supplier shall provide the operator with the public keys, the chain format specification, and the verifier source under terms that survive contract termination.

> **The substrate position the operator should hold is independence from supplier survival. The PQC clauses encode that property contractually.**

13. The transferable artefact

The output of a PQC migration on the AI audit surface is a transferable artefact. The chain file, the public key, the verifier source, and the verdict log together constitute the evidence a sector regulator can walk without operator cooperation. The artefact transfers across regulator engagements, across sector reviews, across contract terminations, across vendor failures.

The artefact is the proof the operator made the migration. It is the single document the regulator asks for at hour zero, and the substrate produces it by construction.

14. Closing

The NCSC roadmap is, in 2026, the operator's compliance horizon. Every AI workload on a CNI estate runs cryptographic primitives somewhere underneath; the operator that has those primitives on PQC today is the operator that walks into 2031 prepared. The substrate is the position underneath the migration, not a feature of the migration.

Engineering leadership at National Grid, SSE, Drax, Centrica, BT, Openreach, Thames Water, Severn Trent, United Utilities, HSBC UK, Barclays, Lloyds Banking Group, NatWest Group, Santander UK, and the wider PRA-regulated and CNI operator community is open to a fifteen-minute substrate briefing at any time. press@mickai.co.uk.

APPENDIX · ABOUT THE AUTHOR

Micky Irons

Founder of Mickai LTD (Companies House 17166618, England and Wales, registered office 20 Wenlock Road, London, N1 7GU). Named inventor on the Mickai SIOS patent corpus, recorded on the UK Intellectual Property Office public register at numbers GB2607309.8 to GB2611702.8 and GB2611885.1 onwards. Trade mark Mickai registered at UK00004373277 (classes 9 and 42, filed 15 April 2026).

Before founding Mickai, Micky was a Sellafield site worker. The egress constraint observed from inside the regulated workstation is the engineering origin of the substrate described across the Mickai ebook series.

Profiles and links

mickai.co.uk · the canonical Mickai site.

crunchbase.com/person/micky-irons · founder profile.

linkedin.com/in/mickyirons · personal LinkedIn.

github.com/Micky-CMO · open-source position.

linkedin.com/company/mickai · Mickai LTD company page.

crunchbase.com/organization/mickyirons · Mickai LTD Crunchbase entry.

Email: press@mickai.co.uk

References and further reading

· NCSC, Timelines for migration to post-quantum cryptography.

· NCSC, Preparing for quantum-safe cryptography (guidance series).

· NIST FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism, August 2024.

· NIST FIPS 204, Module-Lattice-Based Digital Signature Standard, August 2024.

· NIST FIPS 202, SHA-3 Standard, August 2015.

· RFC 8949, Concise Binary Object Representation (CBOR), December 2020.

· DSIT AI Cyber Security Code of Practice (consultation 2024 to 2025).

· PRA Supervisory Statement SS1/23, model risk management principles for banks.

· Mickai Audit Verifier, reference implementation: mickai.co.uk/audit-verifier.

· Mickai OAR Brain documentation: mickai.co.uk/oar.

· Mickai trade mark UK00004373277, classes 9 and 42, filed 15 April 2026.

Colophon

Set in Inter Tight (Variable) and Inter Black. Cover and body chrome in the Mickai gold-on-void palette. Brand voice audited under the Mickai AMT preflight gate; zero violations at publish.

© 2026 Mickai LTD. Reproduction permitted for internal procurement and engineering use within UK regulated organisations. External redistribution by written permission of the author.