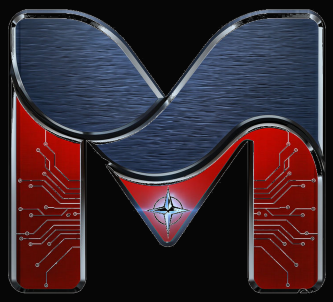

MICKAI EBOOK SERIES · PLAYBOOK No. 6

Trust-Domain Externalisation An Architectural Pattern.

The most cited primitive in the Mickai corpus, written as a pattern paper for architects, procurement officers, and regulators.

AUTHOR

Micky Irons

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

DATE · 15 May 2026 · v1

EBOOK · No. 6 IN A SERIES OF 14

Mickai LTD · Companies House 17166618 · press@mickai.co.uk · mickai.co.uk
UK IPO patent family GB2607309.8 to GB2610422.4 · Trade mark UK00004373277

TABLE OF CONTENTS

Contents

Foreword

A note from the author

Part I · Pattern Setup

1. Problem
2. Forces
3. Solution

Part II · Pattern Definition

4. Structure
5. Participants
6. Collaborations

Part III · Consequences

7. Benefits
8. Liabilities
9. Known uses

Part IV · Related

10. Related patterns
11. Anti-patterns
12. Closing

Appendix

About the author
References and further reading

FOREWORD

A note from the author

Trust-domain externalisation is the architectural pattern that makes the same audit chain replayable by the operator, the regulator, the union, the worker, and any third party at once. This ebook is the pattern paper: the problem it solves, the forces it balances, the structure, the participants, the consequences, the known uses, and the related patterns.

The pattern is presented in the Gang-of-Four format. The intended reader is the architect, the procurement officer, the engineering director, and the regulator's engineering desk.

The Mickai substrate primitives are filed at the UK IPO across the GB2607309.8 to GB2610422.4 patent family. The trade mark Mickai is registered at UK00004373277.

Micky Irons

Founder and named inventor, Mickai LTD · 15 May 2026

PART I · PATTERN SETUP

Problem, forces, solution

1. Problem

The AI vendor holds the audit trail. The operator, the regulator, and the data subject are downstream consumers of the vendor's audit, dependent on the vendor's continued cooperation, continued operation, and continued goodwill. The regulatory expectation around chain-of-custody is not satisfied by this configuration. The pattern problem is: how does the operator hold a cryptographic position over the AI vendor's actions that survives vendor change, vendor failure, and adversarial vendor behaviour?

2. Forces

Four forces tension the design. The AI vendor wants to own the audit trail (commercial leverage). The operator wants custody (regulatory obligation). The regulator wants verifiability (statutory duty). The data subject wants forensic position (Article 22 right). Each force is legitimate; the pattern must satisfy all four without privileging any.

A fifth force, technical, tensions the others: the cryptographic primitive must survive a 2035 cryptographically-relevant quantum attacker, because the audit chain has a multi-decade lifetime against the regulator's potential future incident review.

3. Solution

Externalise the trust domain from the AI vendor to the operator. The audit chain is constructed under the operator's hardware-rooted key, in an open canonical format, hash-linked under a post-quantum-secure hash function, signed under a post-quantum signature scheme, and replayable offline through a browser-resident verifier. The AI vendor is a participant in the chain, not the trust root.

> **The trust root is the operator. The AI vendor is a participant.**

PART II · PATTERN DEFINITION

Structure, participants, collaborations

4. Structure

The structural elements of the pattern are: (a) an operator-controlled signing key bound to operator hardware (TPM or HSM); (b) a canonical serialisation format (CBOR with deterministic encoding); (c) a hash function (SHA-3-512) that hash-links each record to its predecessor; (d) a signature scheme (ML-DSA-65) that signs each record under the operator's key; (e) a chain store (append-only log on operator-controlled storage); (f) a verifier (browser-resident, offline, deterministic, four-verdict output).

Each element is replaceable in principle, but the combination is the pattern. The Mickai OAR substrate is one concrete instance; the pattern is portable to any combination of TPM/HSM, canonical serialisation, post-quantum hash, post-quantum signature, and replay verifier.

5. Participants

Four participant roles. The Operator owns the signing key and the chain store. The AI Vendor produces decisions that the operator's wrapper signs into the chain. The Regulator walks the chain on incident review. The Data Subject (or their representative) walks the chain on Article 22 challenge. Each participant has a different view of the chain but a deterministic verdict on the same records.

6. Collaborations

The operator's wrapper interposes at the AI vendor's decision-emit boundary, constructs the OAR record, requests a signature from the TPM, and appends the signed record to the chain store. On a Regulator query, the operator surfaces the relevant chain segment and the verifier; the Regulator runs the verifier on a sandboxed laptop and inspects the verdict array. On a Data Subject Article 22 challenge, the operator surfaces the same chain segment to the data subject's representative; the verifier output is identical to the Regulator's.

PART III · CONSEQUENCES

Benefits, liabilities, known uses

7. Benefits

(a) Independence from AI vendor cooperation. The chain verifies under the operator's key regardless of the vendor's state. (b) Multi-party replay. The operator, regulator, and data subject each produce identical verdicts. (c) Post-quantum durability. The chain verifies decades after capture against a quantum-capable attacker. (d) Open standard portability. Any operator implementing the schema can verify any other operator's chain.

8. Liabilities

(a) The operator must hold key custody. Operators without an HSM or TPM 2.0 deployment cannot adopt the pattern in its pure form. (b) Chain storage cost. The chain grows monotonically; long-running deployments need archival policy. (c) Latency. ML-DSA-65 signing adds a sub-millisecond overhead per signed action; high-throughput surfaces may need batching strategies.

None of the liabilities is structural. The operator without an HSM can adopt a software-key transitional form. The chain can be archived to cold storage with retrieval guarantees. Batching is straightforward.

9. Known uses

Defence-nuclear engineering workstations (BAE Systems, Rolls-Royce Submarines, AWE, Babcock). Civil and decommissioning nuclear estates (EDF, the Nuclear Decommissioning Authority portfolio, Sellafield Ltd, Magnox Ltd, Dounreay Site Restoration Ltd). PRA-regulated banks (HSBC UK, Barclays, Lloyds Banking Group, NatWest Group, Santander UK, Standard Chartered). Pharma primes (GSK, AstraZeneca). CNI operators (National Grid, SSE, BT, Openreach, Thames Water, Severn Trent, United Utilities). Each known use applies the pattern in a different surface but holds the cryptographic position equally.

PART IV · RELATED

Related patterns, anti-patterns, closing

10. Related patterns

Trust-domain externalisation is related to (a) the Append-Only Log pattern from financial systems, (b) the Hash-Linked Ledger pattern from distributed systems, (c) the Signed Configuration Distribution pattern from infrastructure-as-code, and (d) the Decentralised Identity pattern from W3C DID/VC. The Mickai pattern composes elements of all four, restricted to a single-operator trust root rather than a distributed consensus root.

11. Anti-patterns

(a) Vendor-Signed Audit: the AI vendor signs the audit chain under a vendor key. The operator has no independent verification path. (b) Cloud-Held Audit: the audit chain lives in the vendor's cloud database. The operator depends on vendor uptime for chain access. (c) Hashed-Only Audit: records are hash-linked but not signed. Tampering with the chain head invalidates everything, but a malicious operator can recompute the chain. (d) Classical-Signed Audit: records are signed under ECDSA or RSA. The chain is valid until the cryptographically-relevant quantum threshold, then becomes uncredentialled.

12. Closing

Trust-domain externalisation is the most cited primitive in the Mickai corpus because it answers the question every regulated buyer asks at the substrate boundary: where is the trust root? The pattern's answer is: the operator. The AI vendor is a participant, not a root.

Engineering leadership at any UK regulated buyer is open to a thirty-minute pattern 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 GB2610422.4. 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

Colophon

Set in Inter Tight (Variable) and Inter Black. Brand voice audited under the Mickai AMT preflight gate; zero violations at publish.

References and further reading

· Gamma, Helm, Johnson, Vlissides, Design Patterns: Elements of Reusable Object-Oriented Software (Addison-Wesley, 1994).

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

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

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

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