MICKAI™

MICKAI EBOOK SERIES · PLAYBOOK No. 11

Mickai's Hybrid Sandbox. How a Sovereign AI Reaches the Internet.

A technical walkthrough of the Mickai Browser Brain, the sandboxed network egress model, and the cryptographic boundary that lets a sovereign AI use the Internet without surrendering the operator's trust root.

AUTHOR

Micky Irons

Founder and named inventor, Mickai LTD.

Crunchbase · LinkedIn · GitHub · mickai.co.uk

EBOOK · No. 11 IN A SERIES OF 14

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

DATE · 18 May 2026 · v1

MICKAI™

EBOOK · No. 11 IN A SERIES OF 14

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 Problem

1. Why a sovereign AI needs the Internet
2. Why a vendor-proxied Internet surrenders the trust root
3. The third path: a hybrid sandbox

Part II · The Architecture

4. The Browser Brain
5. The sandboxed egress channel
6. The cryptographic boundary

Part III · Workflows

7. Web research with audit chain
8. Form submission and account access
9. Tool invocation through external APIs

Part IV · Compliance

10. NCSC and the AI Cyber Security Code
11. UK GDPR and outbound data flow
12. Closing

Appendix

About the author
References and further reading

FOREWORD

A note from the author

A sovereign AI that cannot reach the public Internet is functionally crippled. A sovereign AI that reaches the Internet through a vendor-controlled proxy has surrendered the trust root. This ebook is the technical walkthrough of the third path: a hybrid sandbox that gives the AI Internet reach while keeping the cryptographic boundary intact.

The architecture is the Mickai Browser Brain. The sandbox is the operator-controlled boundary that mediates every network call. The substrate is the OAR chain that records every reach.

The Mickai substrate primitives are filed at the UK IPO 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 · 18 May 2026

PART I · THE PROBLEM

Why Internet reach is the hard architectural problem

1. Why a sovereign AI needs the Internet

An AI that cannot reach the public web is limited to its training corpus and the documents the operator hands it. For most operator workflows (research, fact-checking, regulatory monitoring, customer engagement, competitive intelligence) the Internet reach is the variable that decides whether the AI is useful. A sovereign AI that pretends the Internet does not exist is a sovereign AI that does not get deployed.

2. Why a vendor-proxied Internet surrenders the trust root

The default approach to AI Internet reach is to proxy through a vendor's gateway. The vendor signs the TLS connection, the vendor sees the AI's prompts, the vendor logs the AI's queries, and the audit trail of what the AI saw on the Internet is in the vendor's database. The trust root has migrated to the vendor.

For a regulated buyer, the vendor proxy is structurally unacceptable. The substrate question is whether the AI can reach the Internet without transferring the trust root.

3. The third path: a hybrid sandbox

The hybrid sandbox is the third architectural option. The AI emits a network intent, the sandbox mediates the intent against the operator's policy, the sandbox executes the call on the operator's network from the operator's hardware, and the AI receives the response with the call recorded in the OAR chain. The trust root stays on operator iron; the Internet is reached through an operator-controlled boundary.

PART II · THE ARCHITECTURE

Browser Brain, sandboxed egress, cryptographic boundary

4. The Browser Brain

The Browser Brain is one of the twenty-five brains in the Mickai SIOS. It accepts network-reach intents from the Arbiter Brain, applies the operator's network policy from the Policy Brain, executes the resulting calls through a sandboxed browser instance running on the operator's hardware, and emits the response back into the SIOS as a signed OAR record.

The sandboxed browser is a real browser (Chromium or Firefox compiled against the operator's hardened build), running in an isolated process namespace, with network egress restricted to operator-policy-approved hosts.

5. The sandboxed egress channel

Network egress is mediated by an operator-controlled policy. The policy defines allowed hosts, allowed protocols, allowed methods, allowed data classes for outbound payloads, and rate limits. Each network call is checked against the policy before execution; calls that fail policy are recorded as DENIED in the OAR chain and never executed.

The egress channel is observable. Every byte that leaves the operator's perimeter is recorded in the OAR chain along with the destination, the protocol, the response size, and the response status. The operator can replay the chain and reconstruct exactly what the AI sent to the Internet.

6. The cryptographic boundary

The cryptographic boundary is the OAR chain itself. Every browser action emits a record signed under the operator's TPM-bound ML-DSA-65 key. The chain is the operator's evidence of every Internet-reach action the AI has taken. The regulator's chain-of-custody question is answered at the same primitive layer as the rest of the SIOS audit chain.

> **The Internet is reached, but the trust root stays on operator iron.**

PART III · WORKFLOWS

Three concrete workflows on the hybrid sandbox

7. Web research with audit chain

An operator asks the Mickai SIOS to research the 2026 NCSC PQC migration roadmap. The Arbiter dispatches to the Browser Brain. The Browser Brain visits the NCSC site, walks the relevant guidance pages, extracts the relevant sections, signs each visit into the OAR chain, and emits a structured summary back to the Arbiter. Six months later, the operator can replay the chain and inspect exactly which pages the AI visited, at what time, with what response.

8. Form submission and account access

An operator's workflow requires submitting a structured form to a regulator's portal. The Browser Brain accepts the workflow intent, the Policy Brain confirms the destination is policy-approved, the Permissions Brain confirms the operator has authorised this action, the Browser Brain executes the submission, the OAR chain records the submitted payload, the response, and the operator's authorising principal.

9. Tool invocation through external APIs

An operator's workflow requires calling a third-party SaaS API. The Browser Brain executes the call against the operator's API credentials, the credentials are held in the operator's secret store and never leave the boundary, the call is signed into the OAR chain, the response is parsed and emitted to the calling brain. The third-party SaaS sees the operator's IP address and credentials; the AI vendor is not in the call path.

PART IV · COMPLIANCE

NCSC, UK GDPR, and the AI Cyber Security Code

10. NCSC and the AI Cyber Security Code

The NCSC's AI Cyber Security Code of Practice expects AI deployments to have capability scoping, audit logging, and supply chain assurance. The hybrid sandbox satisfies all three at the primitive layer. Capability scoping is the Policy Brain's policy graph; audit logging is the OAR chain; supply chain assurance is the operator's control over the sandboxed browser build, the credential store, and the policy graph.

11. UK GDPR and outbound data flow

UK GDPR's outbound data flow restrictions apply to any personal data the AI sends to the Internet. The hybrid sandbox's data-class policy enforces these restrictions at the egress boundary. Personal data classified as high-sensitivity cannot leave the operator's perimeter through the sandbox unless the destination, the legal basis, and the data class are all policy-approved. The audit chain records every check.

12. Closing

The hybrid sandbox is the answer to the question 'how does a sovereign AI use the Internet?' The trust root stays on operator iron, the policy is enforced at the egress boundary, the audit chain records every reach, and the regulator's chain-of-custody question is answered at the substrate layer.

Engineering leadership at any UK regulated buyer is open to a thirty-minute hybrid-sandbox architectural 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

Colophon

Set in Inter Tight (Variable) and Inter Black. 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.

References and further reading

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

· Information Commissioner's Office, UK GDPR guidance series.

· Mickai brain taxonomy: mickai.co.uk/brains.

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