MICKAI™

MICKAI EBOOK SERIES · No. 16

When Machines Must Explain Themselves.

Explainability, audit and the sealed record that answers the regulator.

AUTHOR

Micky Irons

Founder and named inventor, Mickai LTD.

19 June 2026 · v1 · mickai.co.uk

Mickai LTD · Companies House 17166618 · press@mickai.co.uk · mickai.co.uk
UK IPO register, named inventor Mickarle Wagstaff-Irons · Trade mark UK00004373277

TABLE OF CONTENTS

Contents

FOREWORD

A note from the author

I have spent the last few years building a system that makes machines accountable, and the longer I worked the clearer one thing became. The hard problem in automated decision making is not whether a model can produce an answer. Models produce answers all day. The hard problem is whether anyone can later prove what the machine actually did, why it did it, and that the account has not been quietly edited after the fact. I wrote this book because that gap, the space between an output and a defensible record of the output, is where trust in artificial intelligence is currently breaking.

My name is Micky Irons. I am the founder of Mickai and the named inventor on its filed patent portfolio. Mickai is a Sovereign Intelligence Operating System, which means it runs on the operator's own hardware, stays offline when it needs to, and treats every consequential action as something that must be sealed rather than merely logged. That design choice came from a simple observation. Most AI systems can tell you what they think the answer is. Very few can hand you a record that survives a hostile reader, a regulator, or a courtroom. This book is about closing that distance.

I want to be careful about claims, because the subject deserves care. Some of what I describe is running today. Some of it is designed and filed and not yet in production, and where that is true I say so plainly. The cryptography at the heart of this argument is not mine. The post-quantum signature standard I rely on is a public NIST standard, and I lean on it precisely because it is not a private invention of my own. What is ours is the way the pieces fit together into a sealed record that an outsider can verify without trusting us.

If you regulate AI, build it, buy it, or one day have to defend a decision it made, this book is for you. I have tried to keep it concrete and free of the usual marketing fog. The question underneath all four parts is the same one a judge will eventually ask. When the machine made this decision, what exactly did it do, and how do we know that what you are showing me is true.

Micky Irons

Founder and named inventor, Mickai LTD · 19 June 2026

THE ACCOUNTABILITY GAP

Automated decisions are everywhere, and almost none of them can be proven after the fact.

The decision nobody can reconstruct

Consider an ordinary morning in a large institution. A loan is declined, a benefit is paused, a shipment is rerouted, a patient is flagged for review. Each of these is now routinely decided, or heavily shaped, by an automated system. The person on the receiving end is told a result. They are rarely told the reasoning, and almost never given anything they could take to a third party to check. The decision happened, the consequence is real, and the account of it is thin.

When a complaint arrives weeks later, the institution goes looking for the record. What it usually finds is a scattering of application logs across three services, a model version number that points to an artefact someone has since overwritten, a feature store that was refreshed on its nightly schedule, and a database row that has been updated four times since the decision. Each piece is plausible. None of it, taken together, amounts to proof. The organisation can describe what it believes happened. It cannot demonstrate it in a way that resists a determined challenge.

This is the accountability gap, and it is not a failure of diligence. It is structural. Systems are built to produce outcomes efficiently, not to preserve a defensible account of each outcome at the moment it is made. Storage is treated as a place to look things up, not as evidence. By the time anyone needs the record to mean something, the conditions that produced the decision have moved on, and no amount of good faith can rebuild a state that the system overwrote months ago.

> **An institution can usually describe what it believes happened, but describing is not the same as proving.**

The gap matters more as the stakes rise. A recommendation engine that suggests a film can afford to be opaque, because the worst case is a wasted evening. A system that decides eligibility, risk, or liberty cannot, because the worst case is a person wrongly denied something they were owed and unable to find out why. As automated decisions move into domains with real consequences for real people, the absence of a reconstructable account stops being a technical inconvenience and becomes a question of justice.

Regulators have noticed. The direction of travel across jurisdictions is toward a right to an explanation and a duty to keep records of how high impact systems behave. Articles 13 to 15 and 22 of the General Data Protection Regulation already gesture at this, and the Artificial Intelligence Act sharpens it for high risk systems. The instinct is correct. The difficulty is that most current systems were never built to answer that demand honestly, and retrofitting honesty into an architecture designed only to produce

answers is far harder than it sounds.

Why a log is not provenance

The reflexive answer to the accountability gap is logging. Turn on more logs, keep them longer, and surely the record will be there when it is needed. This is comforting and largely mistaken. A log tells you that a system wrote down a line of text claiming something occurred. It does not tell you that the claim is true, that it is complete, or that nobody has touched it since.

Provenance is a stronger idea than logging. Provenance is an account of origin and history that is bound to the thing it describes, in a way that makes tampering evident. A log is a story the system tells about itself. Provenance is a story that an independent party can check against the cryptographic evidence, without having to take the storyteller's word for it. The difference is the difference between a witness statement and a sealed exhibit.

> **A log is a story a system tells about itself; provenance is a story an outsider can verify without trusting the storyteller.**

Ordinary logs fail three tests that real provenance must pass. They are usually editable by whoever holds the database credentials, so a privileged insider can rewrite history and leave the row looking untouched. They are rarely bound to the exact inputs, model, and parameters that produced a specific decision, so they describe the neighbourhood of the event rather than the event itself. And they carry no cryptographic proof of integrity, so a single altered character leaves no trace. Each failure is fatal in front of someone who is actively looking for a reason to doubt you.

The deeper problem is incentive. The party that holds the logs is very often the party with the most to lose if the logs are unfavourable. We would not accept a defendant grading their own evidence in any other setting, yet in automated decision making we routinely ask the operator of a system to be the sole keeper and editor of the record of what that system did. Provenance exists precisely to remove that conflict, by making the record verifiable by people who do not trust each other and who hold no shared interest in the outcome.

None of this means logs are useless. They are excellent for debugging a failing service at three in the morning and for understanding load patterns over a quarter. They are simply the wrong instrument for accountability, in the same way a hand sketch is the wrong instrument for a legal land survey. When the question is what happened and can you prove it, a log answers the first half and quietly declines the second.

The Mickai pantheon.

Explainability is necessary and not sufficient

Much of the public conversation about trustworthy AI has settled on explainability. We want systems that can articulate why they reached a conclusion, in terms a human can follow. This is a worthy goal and I support it. An explanation that a person can understand is the difference between a decision that can be contested and one that can only be endured. But explainability alone does not close the accountability gap, and it is worth being precise about why.

An explanation is a claim about reasoning. Like any claim, it can be sincere, mistaken, or fabricated. A system can generate a fluent, plausible rationale for a decision that has very little to do with the computation that actually produced the outcome. We have all watched models produce confident narratives that do not match their internal behaviour, and post hoc attribution methods can disagree with each other on the very same prediction. An explanation you cannot bind to the real decision is, at best, a helpful guess and, at worst, a convincing alibi.

> **An explanation you cannot bind to the real decision is at best a helpful guess and at worst a convincing alibi.**

What turns an explanation into evidence is binding. The account of why must be tied, cryptographically and inseparably, to the record of what. The specific inputs, the specific model and version, the specific parameters, the specific output, and the human readable reasoning must travel together as one sealed object, so that you cannot quietly swap the explanation while keeping the outcome, or revise the outcome while keeping the explanation. Without that binding, explainability and accountability drift apart, and a clever operator can offer you whichever one is more flattering.

So I treat explainability as the front of the house and provenance as the foundation. The reasoning should be legible to the person affected, the engineer, and the auditor. Underneath it, sealed and verifiable, must sit the proof that this reasoning belongs to this decision and that neither has been altered. One without the other is half a system, and it is the half the industry has neglected because explanations demonstrate well and seals do not.

That is the problem stated in full. Decisions are automated, records are weak, logs are not provenance, and explanations float free of the events they claim to describe. The rest of the book is about a mechanism that ties these threads into something an institution can actually stand behind, and that an outsider can actually check without being asked to trust the institution first.

THE SEALED RECORD

How the Open Audit Record binds a decision to a signature that cannot be quietly rewritten.

What the Open Audit Record actually seals

Inside Mickai, every consequential action produces an Open Audit Record. I will use the abbreviation OAR throughout. The OAR is not a log line and it is not a summary written after the event. It is a structured object created at the moment of the decision, containing the things you would need to reconstruct and defend that decision later. It exists because I decided early that the record had to be a first class output of the system, not an afterthought bolted on for compliance.

A single record captures the inputs that were presented, the identity and version of the brain that acted, the parameters in force, the output that was produced, and the human readable reasoning that accompanied it. It also captures the context that makes a decision intelligible later, such as the time, the operator, and the chain of prior records the action depended on. The aim is that someone reading the OAR a year afterwards can answer the auditor's question without having to trust that the surrounding systems are unchanged, because the record carries its own evidence rather than pointing at infrastructure that has since moved on.

> **The record had to be a first class output of the system, not an afterthought bolted on for compliance.**

Mickai is built as fifty specialised brains, twenty five of them domain brains and twenty five operational, running on the operator's own hardware and able to work fully offline. When one of those brains takes a consequential action, the OAR records which brain it was and under what configuration. This matters because accountability in a system of many specialised components requires knowing not just that the system acted, but which part of it acted and how it was set up at that instant, so that a fault can be traced to a named component rather than to the system as an undifferentiated whole.

The word open in Open Audit Record is deliberate. The record is structured so that it can be read and checked by tools that are not ours, using a public signature standard that anyone can implement. I did not want a sealed record that only Mickai could open, because a seal only its maker can inspect is not much of a seal. Verifiability by strangers is the whole point, and it is the difference between asking a regulator to trust a vendor and handing them something they can check on their own machine.

There is a discipline that comes with this. If every consequential action must seal a complete record, then the system has to be honest with itself at the moment of acting about what the inputs and reasoning really were. You cannot seal a decision and tidy it up afterwards, because the seal closes over whatever was true at that instant. That constraint is uncomfortable for a builder, and it is exactly

why it produces records you can rely on.

The Mickai pantheon.

FIPS 204 and the post-quantum signature

A record is only as trustworthy as the seal on it. The OAR is signed using a digital signature scheme, and the scheme I rely on is ML-DSA-65, standardised by the United States National Institute of Standards and Technology as FIPS 204. I want to be exact about the provenance of this, because exactness is the whole spirit of the book. FIPS 204 is a public standard. Mickai did not invent it and does not claim to have invented it. We use it because it is independent of us, and because anyone can read the specification and confirm that our seals conform to it.

A digital signature does two things at once. It proves that the record was sealed by the holder of a particular private key, and it proves that the record has not changed by so much as a single bit since it was sealed. Alter any part of a signed OAR, the inputs, the output, the reasoning, even a timestamp, and the signature no longer matches. The tampering is not hidden and apologised for later. It is mathematically obvious to anyone who runs the public verification against the public key.

> **Alter a single bit of a sealed record and the signature stops matching; the tampering becomes mathematically obvious.**

Why post-quantum, and why now

Most signatures in use today rest on mathematics that a sufficiently powerful quantum computer would break. That machine does not exist yet at the scale required, but a record sealed today may need to be defensible in a decade or two, well inside the window where the assumption could fail. An adversary can also store signed records now and attempt to forge or repudiate them later, once the

tools catch up, which is why the threat is not safely deferred to the day a quantum computer arrives. Choosing a post-quantum scheme is therefore not futurism. It is a sober judgement about how long these records have to last.

ML-DSA-65 sits in the middle of the FIPS 204 security parameters, which is a deliberate choice of margin over economy. For a record that may one day be read in a dispute, I would rather carry slightly larger signatures than gamble on the lowest setting holding up across the lifetime of the evidence. The cost is a few kilobytes per record. The benefit is that the seal is built to outlive the cryptographic assumptions of the present decade, which is the only timescale that matters for evidence.

Around the signing sits a set of custody capabilities that the architecture defines and the portfolio describes. Key rotation, trustee succession, a dead man's switch, and post-quantum custody are part of the design. Some of these are designed and filed rather than in production today, and I will not pretend otherwise. The principle they serve is constant. A signature is only as trustworthy as the governance of the key behind it, so the key has to have a defensible life cycle of its own, from the moment it is generated to the moment it is retired or passed on.

Anchoring provenance to Pantheon

A signed record proves that whoever held the key sealed exactly this content. It does not, by itself, prove when the record came into existence, or stop someone with the key from quietly producing a backdated record and claiming it is old. To close that gap you need an independent witness to time and existence. In Mickai that witness is Pantheon.

Pantheon is a sovereign Layer 1 that anchors to Bitcoin. Architecturally it is a base chain together with fifteen application chains, with a fixed supply token, PAN, providing the economic backbone. I should be clear that Pantheon is the part of the wider architecture still being built out, rather than a finished chain I am presenting as complete. The role it plays for accountability is narrow and important. The fingerprints of sealed records are committed onto Pantheon, and because Pantheon in turn anchors to Bitcoin, the existence of a record at a point in time becomes very difficult to deny and very expensive to forge.

> **A signature proves who sealed the record; anchoring to Pantheon proves it existed by a given moment and was never rewritten.**

The combination is what makes the system strong. The post-quantum signature answers who sealed this and has it changed. The anchor answers did this exist by this time and could it have been rewritten since. One without the other leaves a door open. A signature with no anchor can be backdated by its own keyholder. An anchor with no signature commits to a fingerprint of something it cannot prove the content of. Together they pin a record to both an author and a moment, and an opponent has to defeat two independent mechanisms rather than one.

I chose to anchor to Bitcoin through Pantheon rather than to a private ledger we control because, once again, the value lies in independence. A record whose timeline is guaranteed only by the same party that produced it is no stronger than that party's word. By committing the fingerprint to a public, widely witnessed chain, the timeline of the record becomes something no single operator, including us, can quietly revise, because revising it would mean rewriting a chain that thousands of unrelated parties are watching.

That is the mechanism in full. A complete record sealed at the moment of decision, signed with a public post-quantum standard so any change is detectable, and anchored to an independent chain so its existence in time cannot be denied. The next part turns from how it works to why it is worth doing, in evidence and in money.

The Mickai pantheon.

EVIDENCE AND ECONOMICS

What a sealed record is worth when the explanation has to survive scrutiny, and what it costs to skip it.

When the explanation has to survive a courtroom

Imagine the moment this whole apparatus is built for. A decision made by an automated system is disputed, the dispute reaches a tribunal or a court, and the operator is asked to account for what happened. This is the test that strips away marketing. A courtroom is an environment specifically designed to find the weak point in a story, with a motivated opponent looking for any reason to say your record cannot be trusted.

In that room, a pile of application logs is a liability as often as an asset. Opposing counsel will ask who held the credentials to edit them, whether they capture the exact inputs the model saw, and how anyone knows they were not assembled after the complaint arrived. Each question lands because ordinary logs have no good answer to any of them. The operator is reduced to asking the court to trust their internal processes, which is precisely the trust a dispute has called into question.

> **A courtroom is built to find the weak point in a story, with a motivated opponent looking for a reason to doubt your record.**

A sealed OAR changes the posture of that conversation. The record presents a complete account of the decision, carries a signature that demonstrates it has not been altered since sealing, and carries an anchor that places its existence before the dispute began. The questions that destroy a log have clean answers here. Could it have been edited. No, the signature would fail. Could it have been written after the fact. No, the anchor predates the complaint. Is the explanation attached to this actual decision. Yes, it is sealed inside the same record.

I want to be measured about what this does and does not achieve. It does not make a bad decision into a good one. If the system decided wrongly, a sealed record will faithfully prove that it decided wrongly, in full detail, to your own disadvantage. What it does is move the argument from whether the record can be believed to whether the decision was correct, which is the argument that should be had. Honest accountability sometimes convicts you, and a system you trust only when it exonerates you is not an accountability system at all.

This is also why the human readable reasoning has to travel inside the seal. A court does not only want to know what was decided. It wants to know on what basis, in language a person can weigh. By

binding the reasoning to the inputs and the output under one signature, the OAR offers a court both the explanation and the proof that the explanation is the genuine article rather than a tidy reconstruction prepared in the week before the hearing.

The economics of proof

Accountability is often treated as pure cost, a tax that compliance imposes on systems that would rather just run. I think that framing is wrong, and the economics show why. The cost of sealing a record at the moment of decision is small and predictable. The cost of not having a record when you need one is large and arrives at the worst possible time, bundled with legal exposure, regulatory penalty, and reputational damage.

Consider the asymmetry. Sealing an OAR adds a bounded amount of computation and a few kilobytes of storage to each consequential action, paid in small increments as the system runs. The absence of an OAR costs nothing until a dispute, at which point it can cost a settlement, a regulatory fine, the discovery effort of reconstructing events from fragments, and the harder to price loss of being the organisation that could not account for its own decisions. Cheap and steady against rare and ruinous is a trade most risk managers would take in any other domain without a second thought.

> **Sealing is cheap and steady; the absence of a record is rare and ruinous, and it arrives at the worst possible time.**

There is a second economic effect that is easy to miss. A system that can prove its decisions can be trusted with higher stakes work, which is where the value is. An institution that can hand a regulator a verifiable record is in a position to deploy automation into sensitive domains, such as lending, clinical triage, or eligibility, that a less accountable competitor cannot safely enter. Provenance is not only insurance against the bad day. It is a licence to operate where the margins are highest and the barriers to entry keep weaker rivals out.

Running the brains on the operator's own hardware, offline capable, shapes the economics too. Sealing and anchoring happen under the operator's control rather than depending on a third party's continued goodwill or pricing. The operator is not renting their own accountability from a vendor who could raise the price or change the terms at renewal. For an institution that must keep records defensible for years, owning the means of proof is worth more than the apparent convenience of outsourcing it to someone whose incentives may shift.

I will not pretend the economics are weightless. Post-quantum signatures are larger than their classical predecessors, anchoring carries its own modest overhead, and disciplined sealing imposes engineering rigour that some teams will resent. These are real costs. They are also small, knowable, and front loaded, which is exactly the kind of cost a serious organisation should prefer over a large, unknowable liability that detonates during litigation.

The Mickai pantheon.

Sovereignty, patents, and the work in progress

Two further facts shape how seriously a buyer should take all of this, and I want to state them carefully. The first is sovereignty. Mickai is a Sovereign Intelligence Operating System, not an application that phones home. The brains run on the operator's hardware and can work without a connection. That is what makes it possible to promise that the record belongs to the operator, sealed and held under their control, rather than living on infrastructure someone else governs and could withdraw.

The second is the intellectual property position. The architecture is described across a portfolio of one hundred and one filed United Kingdom patent applications, comprising around two thousand two hundred and thirty four claims, owned by Mickai LTD, with the named inventor recorded as Mickarle Wagstaff-Irons. I say filed and I mean filed. These are applications, not grants, and I will not dress them up as anything else. What they represent is a detailed, dated, public account of how the system is meant to work, lodged with a national office on a fixed date that cannot be backdated.

> **These are filed applications, not grants, and I will not dress them up as anything else.**

I am equally careful about the state of the models. Mickai is actively training its own models now, fine tuning and specialising open foundations such as Llama 3.2 and Qwen 2.5, and building a sealed corpus to train on. Funding scales that effort toward fully native weights over time. This is genuine work happening in the present, not a promise deferred entirely to some funded future, and it is also not yet a claim of fully sovereign weights. Both halves of that sentence are true and both belong in an honest account.

The same honesty applies to the custody and continuity features. The dead man's switch, key rotation, trustee succession, and post-quantum custody are part of the designed and filed architecture. Some are operational and some are designed and not yet in production. I keep that line visible on purpose, because a book about machines explaining themselves would be hollow if its author blurred the boundary between what is built and what is planned. The discipline of the OAR is the same discipline I try to apply to my own claims.

That is the evidence and the economics. A sealed record earns its keep in the only room that ultimately matters, it does so at a cost that is small and predictable against a liability that is large and sudden, and it sits inside a system whose ownership and limitations I have tried to state without inflation. The final part turns to what a reader should actually do with all of this.

WHAT TO DO NOW

Practical steps for regulators, builders, and buyers who have to live with automated decisions.

For the regulator

If you write or enforce rules for automated decisions, the most useful shift you can make is to ask for verifiable records rather than mere records. The wording matters. A requirement to keep logs invites the weakest possible compliance, a folder of editable text that satisfies the letter and none of the spirit. A requirement that records be tamper evident and independently verifiable raises the floor to something that actually protects the people the rule exists for.

I would encourage regulators to lean on public standards rather than bespoke schemes. When a standard such as FIPS 204 already exists and is widely scrutinised, a rule that points to that kind of independent benchmark is more durable than one that invents its own. It also prevents the quiet capture that happens when each vendor is allowed to define what accountable means for its own product. Ask for proofs an outsider can check, against standards an outsider can name without the vendor in the room.

> **Require records that an outsider can verify against standards an outsider can name, not folders of editable text.**

A second principle worth encoding is the separation between the party that makes a decision and the party that can vouch for the record of it. Anchoring to an independent ledger is one way to achieve this, but the underlying point is broader. Wherever possible, the proof that a decision happened as described should not rest solely on the word of the organisation that made it. Build that independence into the expectation, and the whole ecosystem improves because no operator can mark its own homework.

Finally, I would urge proportionality. Not every automated action deserves a sealed, anchored record, and a rule that demands one for trivial decisions will be ignored or gamed. The discipline should bite hardest where consequences are highest, in eligibility, risk, safety, and liberty. Reserve the heavy machinery of provenance for the decisions that can ruin someone's day, and the requirement stays credible, enforceable, and worth the cost it imposes.

The Mickai pantheon.

For the builder

If you build these systems, the single most consequential decision is architectural and it has to be made early. Treat the audit record as a first class output of every consequential action, designed in from the start, not a layer you add once the product works. Retrofitting honest provenance onto a system that was built only to produce answers is painful and partial. Building it in from the first line is merely disciplined.

Be precise about what you seal. The record has to bind the inputs, the model identity and version, the parameters, the output, and the human readable reasoning into one object, so that no part can be swapped while the rest stays put. The most common mistake I see is sealing the output but not the explanation, which leaves exactly the gap that lets a plausible rationale be substituted later. Seal the why together with the what, or do not bother.

> **Seal the why together with the what, or do not bother; an unbound explanation is the gap an opponent walks through.**

On cryptography, resist the urge to invent. Use a public, standardised signature scheme and choose your parameters for the lifetime of the evidence rather than the convenience of today. A post-quantum scheme is the responsible default for records that must survive into a future where current assumptions may not hold. The point of using a standard is that your users do not have to trust you about the mathematics. They can trust the published specification and verify against it with code you did not write.

Govern the key as carefully as the record

A signature is only as good as the custody of the key behind it. Plan for rotation, for succession when a key holder is gone, and for continuity if the operator changes or disappears. These are unglamorous and they are where real systems fail, because a leaked or orphaned key quietly undermines every seal it ever made. In Mickai these capabilities are part of the designed and filed architecture, and I keep an honest line between what is operational and what is planned. Hold yourself to that same line in your own claims, because a system that exaggerates its own custody has already failed the test the book is about.

For the buyer, and a closing word

If you buy or deploy automated decision systems, you hold more power over this market than you may realise. Vendors build what buyers insist on. Ask any system you are evaluating a small set of pointed questions and the quality of the answers will tell you almost everything. Can you produce a complete, sealed record of a single decision. Is the explanation bound to the inputs and the output, or merely stored nearby. What signature standard seals it, and can I verify it with tools that are not yours.

Press on independence. Where does the proof of timing come from, and could you, the vendor, quietly backdate a record if you chose to. A vendor who can answer that the timeline is anchored to a public, independent chain is offering you something a vendor relying on their own database cannot. Press on ownership too. Do the records live under my control, on my hardware, or am I renting my own accountability from you on terms you can revise at the next renewal.

> **Vendors build what buyers insist on, so insist on records you can verify, on hardware you control, against standards you can name.**

Reward honesty about limitations rather than punishing it. A vendor who tells you plainly which capabilities are operational and which are designed and filed but not yet in production is showing you the exact discipline you want in the records the system produces. A vendor who claims everything is finished and flawless is telling you how they will describe their failures later. The candour of the sales conversation is a preview of the candour of the audit trail.

I built Mickai because I believe the era of automated decisions you cannot interrogate is ending, and that it should. The technology to make machines account for themselves exists, it rests on public standards rather than private magic, and it costs far less than the disputes it forecloses. What has been missing is the will to treat the record as seriously as the result. That is a choice, and it is available to any regulator, builder, or buyer reading this.

So I will close where I began. One day a person will be harmed by a decision a machine made, and someone will have to stand up and account for it. When that day comes, the only thing that will hold is a record that was sealed at the moment of the decision, signed in a way that makes tampering obvious, and anchored in a way that no single party can rewrite. Build that record now, before you need it, because by the time you need it, it is already too late to make one that anybody should believe.

The Mickai pantheon.

APPENDIX · ABOUT THE AUTHOR

Micky Irons

Founder and chief executive of Mickai LTD (Companies House 17166618, registered office 20 Wenlock Road, London, N1 7GU) and named inventor on the Mickai SIOS patent corpus: 101 filed UK patent applications, around 2,234 claims. Trade mark Mickai registered at UK00004373277.

Profiles

mickai.co.uk

crunchbase.com/person/micky-irons

linkedin.com/in/mickyirons

References and further reading

· National Institute of Standards and Technology, FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA), U.S. Department of Commerce, 2024.

· National Institute of Standards and Technology, Report on Post-Quantum Cryptography, NIST Internal Report 8105, 2016.

· European Parliament and Council, Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024.

· European Parliament and Council, General Data Protection Regulation, Articles 13 to 15 and 22 on automated decision making and the right to information, 2016.

· Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

· Christoph Molnar, Interpretable Machine Learning: A Guide for Making Black Box Models Explainable, second edition, 2022.

· Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley and Sons, 1996.

· Mickai LTD, filed United Kingdom patent applications describing the Sovereign Intelligence Operating System and the Open Audit Record, named inventor Mickarle Wagstaff-Irons, 2024 to 2026.