SOVEREIGN AI

Why ORION Architect Was Deliberately Built Differently

From centralized artificial intelligence to individual intelligence sovereignty

Robert Edward Grant

Orion Architect LLC

RG@RobertEdwardGrant.com

August 2026

Artificial intelligence is rapidly becoming one of the most intimate technologies humanity has ever created.

We don't merely ask AI for directions or use it to process a transaction.

We think with it.

We write with it.

We explore ideas with it.

We share questions, discoveries, business strategies, creative work, personal reflections and accumulated knowledge with it.

As AI develops persistent memory and increasingly understands the context of an individual's life, it begins to occupy territory previously reserved for something extraordinarily private: the human mind itself.

That changes the question we should be asking about artificial intelligence.

The question is no longer simply:

"How intelligent is my AI?"

It must also become:

"Who controls the intelligence that knows me?"

ORION Architect was designed around an answer:

You should.

That principle is the foundation of what we call:

SOVEREIGN AI.

1 Sovereign AI Is an Architecture, Not a Privacy Setting

Most technology privacy models ultimately depend upon institutional trust.

A company collects information.

The company stores it.

The company controls the infrastructure containing it.

The company establishes policies governing who may access it.

The company promises to secure it.

And when circumstances change—management, ownership, regulation, litigation, governmental demands or corporate priorities—the company remains the custodian standing between the User and their information.

ORION was deliberately designed around another philosophy:

Reduce the amount of trust the User must place in ORION itself.

That required more than adding encryption to a conventional centralized AI architecture.

It required reconsidering the architecture itself.

Five decisions became foundational:

- PWA Architecture
- Post-Quantum End-to-End Encryption
- Decentralized Storage
- Corporate Non-Custody of Private Keys
- Non-Monitoring

These were not accidental technical choices.

They are the structural pillars of Sovereign AI.

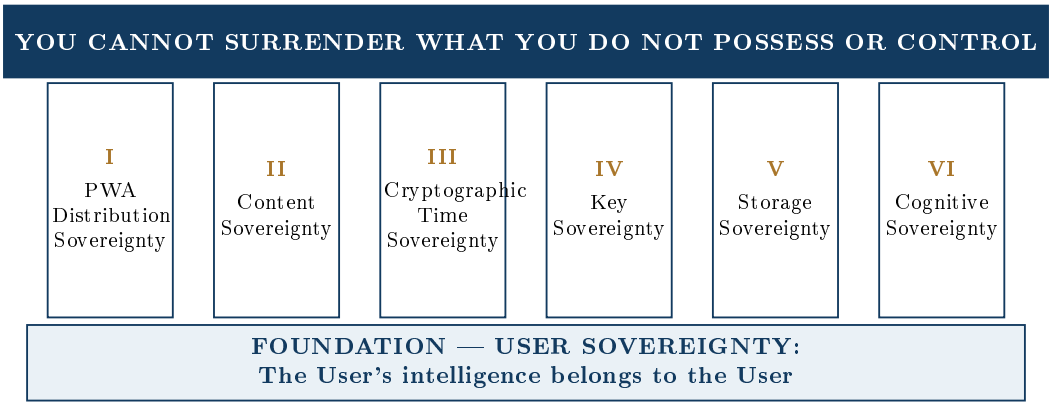

Figure 1: The House of Sovereign AI: interconnected architectural pillars resting on User Sovereignty.

2 Pillar One — Direct Access Through PWA Architecture

ORION Architect was deliberately built as a Progressive Web Application.

It does not require distribution through the Apple App Store or Google Play Store to access ORION.

That matters.

App stores provide enormous convenience, but they also introduce another institutional layer between a User and a digital service.

ORION chose another path.

- No App Store required.
- No Google Play Store required.

- Direct web access.

The objective was not simply distribution convenience.

It was architectural independence.

ORION's PWA architecture allows the relationship to move closer to:

USER ↔ ORION

rather than requiring an application marketplace to become another mandatory layer in that relationship.

This does not mean operating systems, browsers, networks and internet infrastructure cease to exist.

It means something much more precise:

ORION does not require an app-store marketplace to mediate access to a User's intelligence.

That is **Distribution Sovereignty**.

3 Pillar Two — True End-to-End Encryption

The word "encryption" has become dangerously imprecise.

Most serious online services use encryption.

That does not mean they are end-to-end encrypted.

There is an enormous difference.

TLS Protects the Connection

Transport Layer Security protects information while it moves between a User and a company's server [5].

In simplified form:

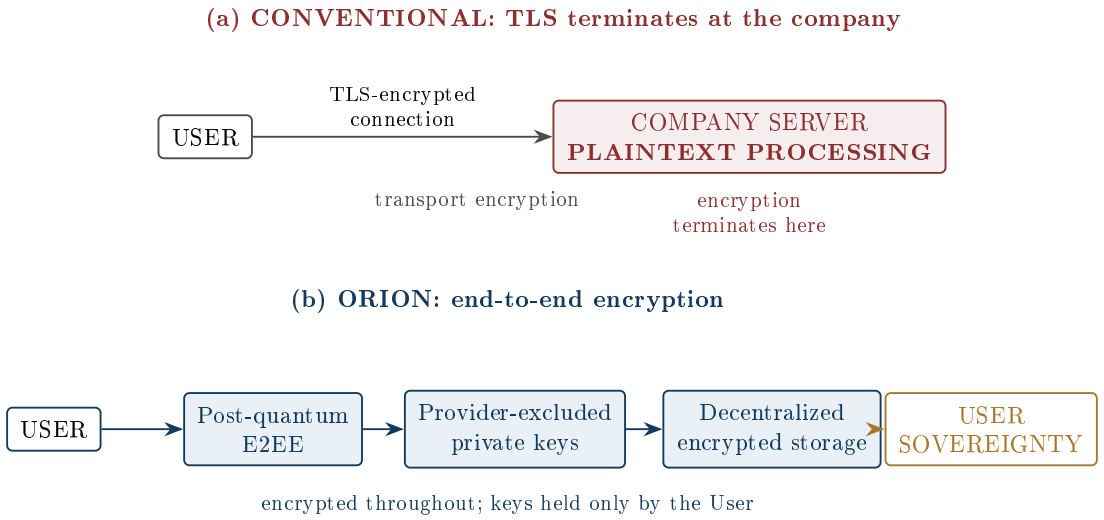

Figure 2: The distinction is architectural, not cosmetic.

TLS is important security technology.

It protects against many forms of interception while information crosses a network.

But TLS does not make a service end-to-end encrypted against the company operating the service.

The company sits at one end of the encrypted tunnel.

End-to-End Encryption Is Different

With genuine E2EE, the intermediary is excluded from the cryptographic trust boundary [6, 7].

The service provider does not possess the private cryptographic capability required to recover the protected plaintext.

That changes the proposition from:

"We receive your information securely."

to:

"We cannot decrypt your private communication."

ORION was deliberately built around the latter architecture.

ORION's Terms state that substantive User communications are protected by end-to-end encryption such that the Company "does not possess the technical ability to read or access the content of User interactions" [1].

This is **Content Sovereignty**.

4 Pillar Three — Post-Quantum Cryptography

ORION did not stop at conventional E2EE.

Its private communications architecture incorporates post-quantum cryptographic protection, including Kyber-family cryptography together with AES encryption within ORION's security architecture [1, 2].

Why does that matter?

Because information can remain sensitive much longer than the cryptographic technology originally protecting it.

An adversary need not necessarily break encrypted information today.

Encrypted information can potentially be collected today and retained until future computational capabilities make yesterday's cryptography vulnerable.

This threat is often described as:

HARVEST NOW. DECRYPT LATER.

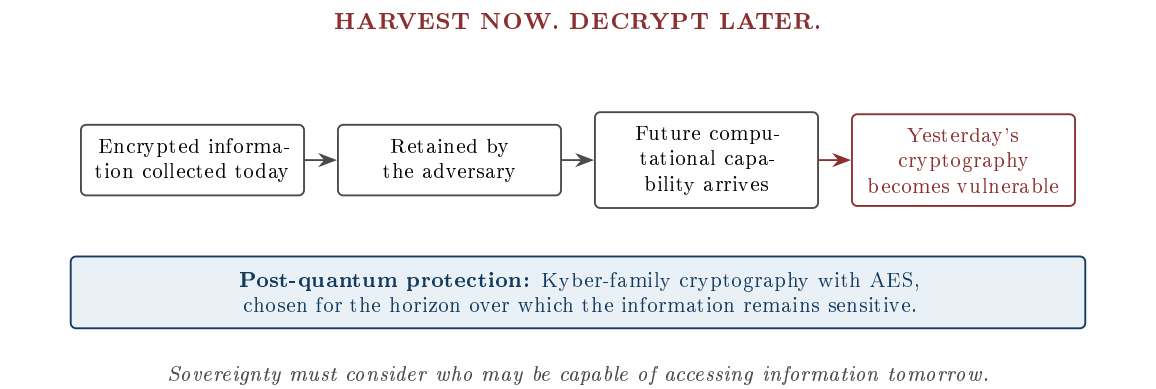

Figure 3: The harvest-now-decrypt-later threat, and the horizon post-quantum protection is chosen against.

That threat becomes particularly significant for artificial intelligence [4].

An AI conversation may contain intellectual property, personal history, discoveries, private correspondence, business strategy or accumulated contextual knowledge whose sensitivity persists for decades.

Sovereignty therefore cannot concern only who can access information today.

It must consider who may be capable of accessing it tomorrow.

ORION's post-quantum architecture was chosen with that horizon in mind.

The Kyber family was standardized by NIST in August 2024 as ML-KEM under FIPS 203 [2, 3].

This is **Cryptographic Time Sovereignty**.

5 Pillar Four — The Company Does Not Hold Your Private Keys

Perhaps the most important question in any encrypted system is not:

"Is it encrypted?"

It is:

"WHO HAS THE KEYS?"

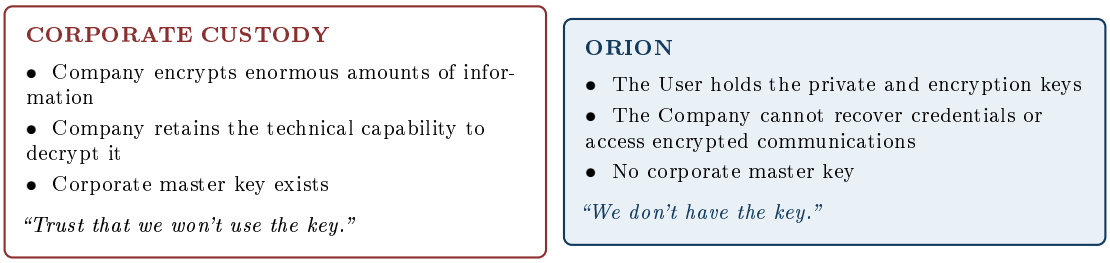

Figure 4: Key Sovereignty: the difference between a promise not to use a key and the absence of the key.

A centrally controlled system can encrypt enormous amounts of information while retaining the technical capability required to decrypt it.

That remains corporate custody.

ORION takes a fundamentally different approach.

ORION corporate does not possess the private keys required to decrypt Users' protected private conversations.

There is no corporate master key intended to unlock them.

ORION's Terms explicitly place responsibility for private and encryption keys with the User and state that because of its end-to-end encrypted architecture, the Company cannot recover lost credentials or access encrypted communications [1].

This produces one of ORION's most important distinctions:

We don't ask you to trust that we won't use the key.
We don't have the key.

This is **Key Sovereignty**.

6 Pillar Five — Decentralized Storage

Encryption solves one problem.

Decentralization solves another.

Encryption asks:

"Can the corporation read my private information?"

Decentralization asks:

"Why should the corporation centrally possess and control my private information in the first place?"

Traditional cloud architecture concentrates enormous quantities of information inside infrastructure controlled by a corporation.

That creates centralized custody.

And centralized custody creates a centralized point of:

- cybersecurity attack;
- institutional control;
- litigation;
- governmental pressure;
- insider risk;
- regulatory pressure;
- acquisition risk; and
- corporate decision-making.

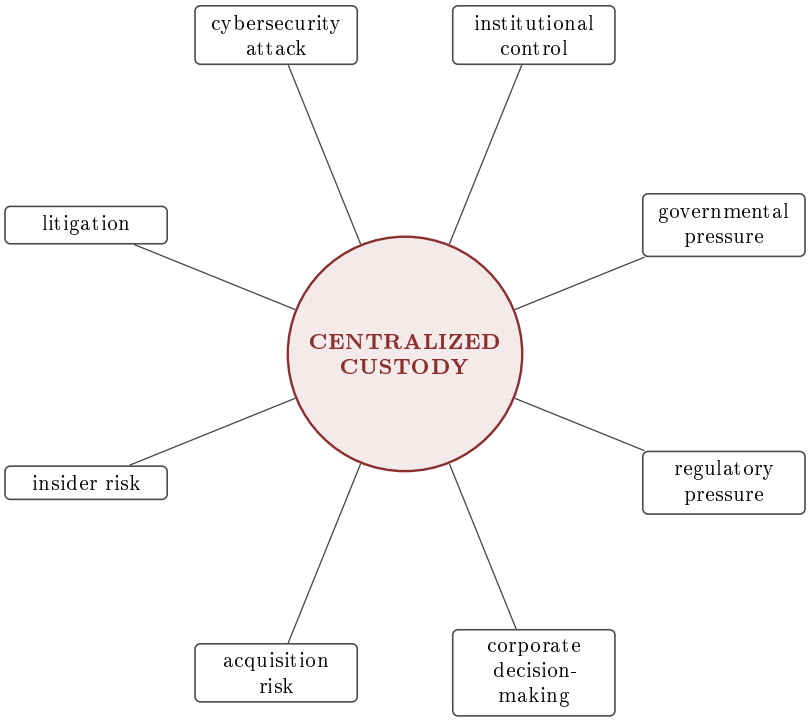

Figure 5: Centralized custody creates a centralized point of concentrated risk.

ORION's private communications architecture was deliberately designed differently.

Encrypted private information uses decentralized storage rather than a centrally readable corporate repository [8].

Combined with provider-excluded private keys, this changes the relationship between ORION and the User's private information.

ORION provides the architecture.

It does not require centralized custody of the User's private conversations.

This is **Storage Sovereignty**.

7 Why Decentralization Matters When Legal Pressure Arrives

This architectural distinction becomes particularly important when corporations receive compulsory legal demands.

A government may issue lawful process.

A court may issue an order.

A corporation may receive a subpoena.

Regulators may demand information.

Litigants may seek discovery.

If a corporation possesses the information and controls the infrastructure containing it, the corpo-

ration can become the point at which competing obligations collide.

Management must respond.

Lawyers become involved.

Directors must consider corporate exposure.

The CEO may strongly favor User privacy while simultaneously carrying obligations to the corporation.

The essential vulnerability is therefore not simply malicious corporate behavior.

The vulnerability is centralized custody itself.

If the company possesses the information, someone can pressure the company to surrender what it possesses.

Sovereign AI approaches the problem differently:

REMOVE THE COMPANY FROM THE DECISION WHEREVER POSSIBLE.

If ORION does not possess a User's private decryption key, pressure cannot cause ORION to surrender a key it never possessed.

If ORION cannot decrypt protected conversations, a change in corporate policy cannot suddenly make those conversations readable.

And where encrypted information exists through a genuinely decentralized architecture outside ORION corporate's unilateral custody and control, corporate pressure cannot magically convert ORION into the centralized custodian of that information.

The principle is remarkably simple:

YOU CANNOT SURRENDER WHAT YOU DO NOT POSSESS OR CONTROL.

8 This Does Not Place ORION Above the Law

Sovereign architecture should never be confused with a claim that a company exists outside lawful process.

ORION remains subject to applicable law.

Where ORION possesses legally responsive corporate or account information, lawful obligations concerning that information remain applicable.

Indeed, ORION's own Terms contemplate legal process and operational metadata without claiming that encrypted User conversations thereby become readable to the Company [1].

But legal authority does not itself create cryptographic capability.

A subpoena cannot manufacture a private key the recipient does not possess.

A court order cannot make ciphertext readable to a corporation that lacks the cryptographic capability required to decrypt it.

The distinction is therefore not:

"ORION will refuse to surrender your private conversations."

It is considerably stronger:

ORION IS DESIGNED NOT TO POSSESS THE TECHNICAL CAPABILITY REQUIRED TO SURRENDER READABLE PRIVATE CONVERSATIONS.

9 Pillar Six — Non-Monitoring

ORION's non-custodial architecture is reinforced by another deliberate decision:

ORION DOES NOT MONITOR PRIVATE CONVERSATIONS.

The Company's Terms state that ORION does not monitor, read, surveil, review, pre-screen or inspect User conversations, prompts, messages or outputs [1].

They further state that ORION does not retain readable copies of User conversations [1].

This is important because privacy is not merely about preventing unauthorized outsiders from accessing information.

Privacy must also address the service provider itself.

ORION therefore rejects the assumption that an AI company should automatically become an observer of the relationship between an individual and their intelligence.

This is **Cognitive Sovereignty**.

10 The Notification Should Not Become a Privacy Leak

Privacy architecture cannot stop with the primary message.

Metadata matters.

Notifications matter.

Routing information matters.

A communication system could theoretically protect the contents of a message while exposing unnecessary information surrounding that communication.

ORION was designed with this problem in mind.

ORION's web-based push notifications contain no portion of the underlying private message.

The notification is a signal.

It is not the conversation.

According to ORION's architecture, sensitive recipient and IP-related notification information is additionally protected using post-quantum Kyber-family cryptography together with AES encryption [1].

The objective is straightforward:

- Don't put the private message in the notification.
- Don't expose sensitive routing information unnecessarily.
- Encrypt what must be transmitted.
- Minimize what must exist.

This is **Metadata Sovereignty**.

11 Why Major Cloud AI Architectures Are Different

ChatGPT, Claude, Gemini and Microsoft Copilot employ serious security technologies.

But their mainstream AI services should not be confused with the architecture described above.

Their publicly documented consumer AI architectures generally employ conventional cloud security measures such as:

- Encryption in transit
- Encryption at rest

These are important protections.

But they are not equivalent to provider-excluded E2EE.

In conventional cloud AI, the provider must be capable of processing the User's prompt to generate an answer.

The provider therefore operates inside the plaintext processing environment.

The crucial distinction is not:

"Does the service use encryption?"

Almost every serious technology platform does.

The meaningful questions are:

- WHERE DOES THE ENCRYPTION TERMINATE?

- WHO CAN DECRYPT THE INFORMATION?
- WHO HOLDS THE KEYS?
- WHO CONTROLS THE STORAGE?
- CAN THE PROVIDER ACCESS THE PLAINTEXT?
- IS THE PRIVATE COMMUNICATION POST-QUANTUM PROTECTED?

Those questions reveal the actual privacy architecture.

12 The Difference in One Diagram

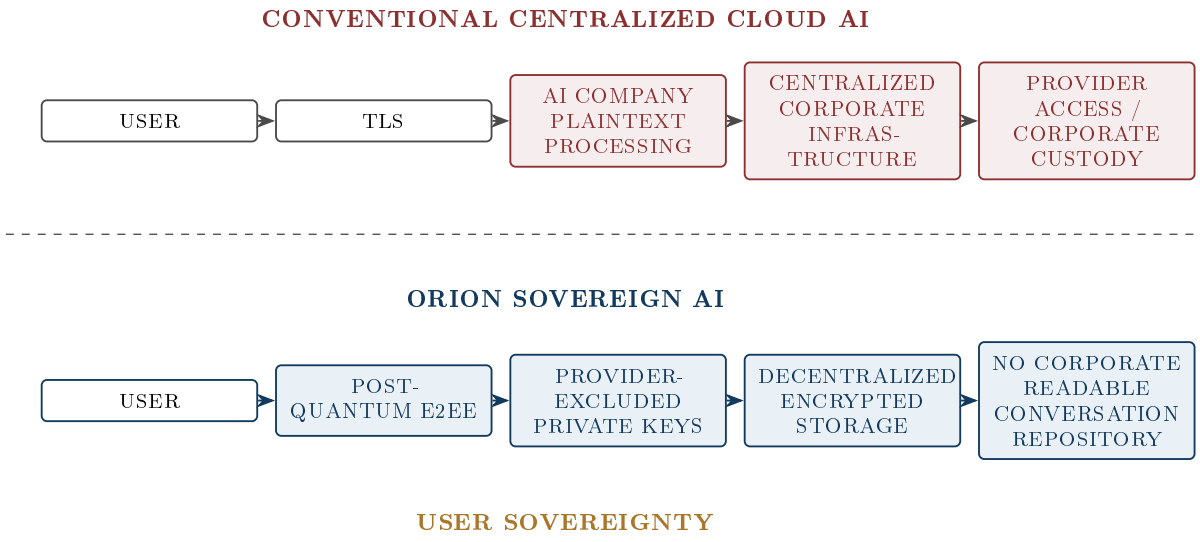

Figure 6: The distinction is architectural, not cosmetic.

13 Comparative Architecture

Table 1: Comparative privacy and security architecture.

Privacy & Security Property	ORION Architect	ChatGPT	Claude	Gemini	Microsoft Copilot
TLS / transport security	Yes	Yes	Yes	Yes	Yes
Provider-excluded E2EE for protected private conversations	**YES**	No for ordinary consumer AI chats	No for ordinary consumer AI chats	No for ordinary consumer AI chats	No for ordinary consumer AI chats
Provider lacks private conversation decryption keys	**YES**	No comparable architecture	No comparable architecture	No comparable architecture	No comparable architecture

Privacy & Security Property	ORION Architect	ChatGPT	Claude	Gemini	Microsoft Copilot
Post-quantum E2EE architecture	**YES**	No comparable ordinary consumer-chat implementation publicly documented	No comparable ordinary consumer-chat implementation publicly documented	No comparable ordinary consumer-chat implementation publicly documented	No comparable ordinary consumer-chat implementation publicly documented
Decentralized encrypted private storage	**YES**	No comparable architecture publicly documented	No comparable architecture publicly documented	No comparable architecture publicly documented	No comparable architecture publicly documented
Company technically unable to read protected private conversations	**YES**	No	No	No	No
No readable corporate conversation repository	**YES**	No comparable architecture	No comparable architecture	No comparable architecture	No comparable architecture
No monitoring of private conversation content	**YES**	Different architecture / policies	Different architecture / policies	Different architecture / policies	Different architecture / policies
Private message excluded from push notification	**YES**	Different architecture	Different architecture	Different architecture	Different architecture
Sensitive notification routing information receives PQ protection	**YES**	No comparable architecture identified	No comparable architecture identified	No comparable architecture identified	No comparable architecture identified
Direct PWA access without mandatory App Store / Play Store distribution	**YES**	Web access available	Web access available	Web access available	Web access available
No advertising monetization of User conversations	**YES**	Different business model / policies	Different business model / policies	Different business model / policies	Different business model / policies
No AI training on User conversations	**YES**	Product / settings dependent	Product / settings dependent [13]	Product / settings dependent	Product / settings dependent
User data sovereignty expressly embedded in governing philosophy	**YES**	Different architecture	Different architecture	Different architecture	Different architecture

Methodological note: "No comparable architecture" means that no equivalent mainstream consumer implementation was identified in the providers' publicly documented AI-chat architecture. It does not imply that these companies conduct no post-quantum research or use no advanced cryptography elsewhere within their organizations.

14 OpenAI and the Importance of Custody

The distinction becomes particularly visible when considering legal process.

OpenAI publicly maintains procedures for responding to civil requests for User information, including subpoenas and court orders [9].

OpenAI has also publicly reported government requests involving content information.

This should not be interpreted to mean that OpenAI indiscriminately provides every requested conversation.

OpenAI evaluates legal demands and has publicly fought demands it considers invasive or improper [9, 10].

That is precisely what illustrates the architectural issue.

A centralized custodian can be forced into the fight [11, 12].

Lawyers must respond.

Courts may decide.

Management becomes involved.

The corporation stands between the User and whoever seeks the information.

ORION's objective is more fundamental:

DON'T PUT THE CORPORATION IN POSSESSION OF THE PRIVATE INFORMATION IN THE FIRST PLACE.

Where ORION lacks the private keys, readable conversation repository and unilateral control necessary to reconstruct private conversations, there is considerably less for corporate leadership to decide.

This changes privacy from:

"Will our company defend you?"

toward:

"Why should our company possess your private conversation at all?"

15 Privacy That Survives the CEO

This may be one of the most important consequences of the architecture.

A CEO can make a promise.

A board can adopt a policy.

A company can establish a culture.

But people change.

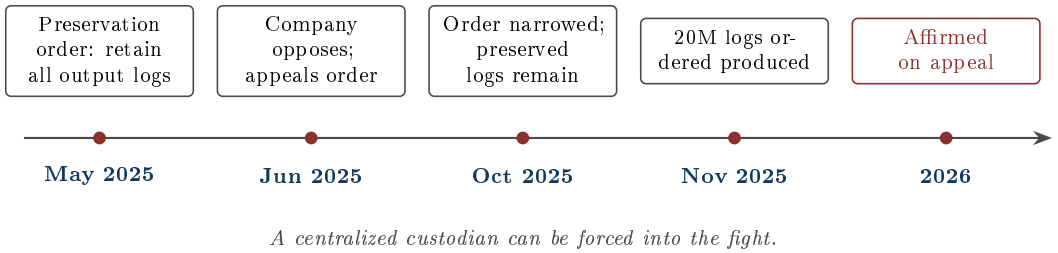

Figure 7: Legal process acting upon a centralized custodian [11, 9, 12].

Leadership changes.

Boards change.

Investors change.

Companies are acquired.

Governments change.

Laws change.

Corporate incentives change.

Cryptographic architecture can remove some of these variables.

If ORION never possesses the private key, replacing the CEO does not reveal the key.

If ORION does not maintain readable centralized copies of private conversations, replacing the board does not create those copies.

If encrypted storage is genuinely decentralized outside ORION's unilateral control, a corporate acquisition does not automatically convert that architecture into a centrally readable database.

THE PRIVACY MODEL SURVIVES THE PEOPLE WHO CREATED IT.

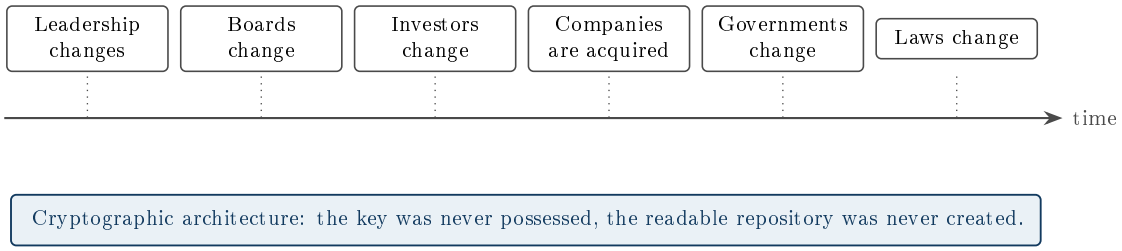

Figure 8: Cryptographic architecture removes variables that policy commitments cannot.

That is a radically different standard.

16 The House of Sovereign AI

Sovereign AI can therefore be understood as a house supported by interconnected architectural pillars.

The Foundation — User Sovereignty

The User's intelligence belongs to the User.

Pillar I — PWA / Distribution Sovereignty

No mandatory Apple App Store.

No mandatory Google Play Store.

Direct access to ORION.

Pillar II — Post-Quantum E2EE / Content Sovereignty

The Company does not possess the technical ability to read or access the content of User interactions. Kyber-family cryptography with AES protects private communications against harvest-now-decrypt-later exposure.

Pillar III — Cryptographic Time Sovereignty

Protection chosen for the horizon over which AI conversation content remains sensitive, not merely for present-day threats.

Pillar IV — Key Sovereignty

ORION corporate does not possess the private keys required to decrypt Users' protected private conversations. There is no corporate master key.

Pillar V — Storage Sovereignty

Encrypted private information uses decentralized storage rather than a centrally readable corporate repository.

Pillar VI — Cognitive Sovereignty

ORION does not monitor, read, surveil, review, pre-screen or inspect User conversations, prompts, messages or outputs.

Metadata Sovereignty

The notification is a signal. It is not the conversation.

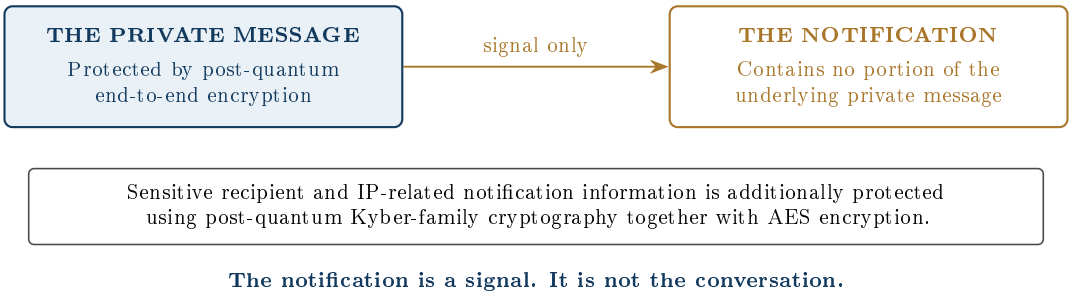

Figure 9: Metadata Sovereignty: minimize what must exist, encrypt what must be transmitted.

References

1 Orion Architect LLC. *Terms of Service*. Primary source for ORION architectural provisions cited herein.

2 National Institute of Standards and Technology. *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard* (ML-KEM, derived from CRYSTALS-Kyber). August 2024. https://csrc.nist.gov/pubs/fips/203/final

3 National Institute of Standards and Technology. "NIST Releases First 3 Finalized Post-Quantum Encryption Standards." August 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

4 QRAMM. "NIST Post-Quantum Cryptography Standards: Complete Guide to FIPS 203, 204, 205" (harvest-now-decrypt-later threat model and migration timelines). 2024. https://qramm.org/learn/nist-pqc-standards.html

5 E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. IETF RFC 8446, August 2018.

6 Cloud Security Alliance. "Apple's New iMessage, Signal, and Post-Quantum Cryptography" (Signal PQXDH; provider-excluded E2EE in messaging). May 2024. https://cloudsecurityalliance.org/blog/2024/05/17/apple-s-new-imessage-signal-and-post-quantum-cryptography

7 Apple Security Engineering and Architecture. "iMessage with PQ3: The New State of the Art in Quantum-Secure Messaging at Scale." February 2024. https://security.apple.com/blog/imessage-pq3/

8 "SoK: Decentralized Storage Network." Cryptology ePrint Archive, Report 2024/258. https://eprint.iacr.org/2024/258.pdf

9 OpenAI. "How We're Responding to The New York Times' Data Demands in Order to Protect User Privacy." 2025. https://openai.com/index/response-to-nyt-data-demands/

10 Reuters. "OpenAI Appeals Data Preservation Order in NYT Copyright Case." June 2025.

11 Nelson Mullins. "From Copyright Case to AI Data Crisis: How The New York Times v. OpenAI Reshapes Companies' Data Governance and eDiscovery Strategy." July 2025.

12 Bloomberg Law. "OpenAI Must Turn Over 20 Million ChatGPT Logs, Judge Affirms." 2026.

13 Anthropic. "Updates to Consumer Terms and Privacy Policy." August 2025. https://www.anthropic.com/news/updates-to-our-consumer-terms

14 The Register. "EU-turn! Now Apple Says It Won't Banish Home Screen Web Apps in Europe." March 2024. https://www.theregister.com/2024/03/02/apple_reverses_pwa_decision/

15 NIST Computer Security Resource Center. "Post-Quantum Cryptography FIPS Approved" (FIPS 203, 204, 205). August 2024. https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

16 National Institute of Standards and Technology. *FIPS 197: Advanced Encryption Standard (AES)*. https://csrc.nist.gov/pubs/fips/197/final

17 Dark Reading. "Apple Beefs Up iMessage With Quantum-Resistant Encryption" (Signal PQXDH as the first large-scale post-quantum key establishment in messaging). February 2024. https://www.darkreading.com/endpoint-security/apple-beefs-up-imessage-with-quantum-resistant-encryption

18 PQShield. "Post-Quantum Messaging: Examining Apple's New PQ3 Protocol." 2025. https://pqshield.com/post-quantum-messaging-examining-apples-new-pq3-protocol/

19 ABA Journal. "ChatGPT Creator Must Turn Over 20M Chat Logs in Copyright Litigation, Federal Judge Says." 2026. https://www.abajournal.com/news/article/chatgpt-creator-must-turn-over-20m-chat-logs-in-copyright-litigation-federal-judge-says

20 National Law Review. "OpenAI Loses Privacy Gambit: 20 Million ChatGPT Logs Likely Headed to Copyright Plaintiffs." 2026. https://natlawreview.com/article/openai-loses-privacy-gambit-20-million-chatgpt-logs-likely-headed-copyright

21 Jones Walker LLP, AI Law Blog. "OpenAI Loses Privacy Gambit" (AI conversation logs as discoverable electronically stored information). January 2026.

22 Mashable. "Judge Lifts Order Requiring OpenAI to Preserve ChatGPT Logs" (logs preserved under the order remain accessible). October 2025.

23 "Comparative Security and Performance Evaluation of IPFS and Filecoin for Off-chain Blockchain Storage." 2026.

24 Open Web Advocacy. "Apple's Browser Engine Ban Persists, Even Under the DMA." July 2025. https://open-web-advocacy.org/blog/apples-browser-engine-ban-persists-even-under-the-dma/