0DATA LAB · PAPER 009 · JULY 2026

The Symbiotic Internet

Toward a Vertebrate Network

Hadda TIKIJJA

0DATA Lab, Rennes, France

Series: Foundations of Digital Organisms · Paper 009

ABSTRACT

Today's Internet is a jellyfish — a network without a spine, where data belongs to platforms, where identity is proven by password, and where every threat must be fought thousands of times in parallel. We describe the Symbiotic Internet: a network where every packet carries a readable intent, every node verifies the Law without a central authority, and every threat, once seen, is remembered forever. A network where platforms become interfaces once again — windows onto your data, not prisons that lock it away. Where spam is technically impossible. Where phishing dies before reaching your inbox. We show how SPINA serves as the backbone of this network, how the capability manifest makes every graft readable, and how a gateway — the Airlock — enables coexistence with today's Internet without rupture. This is not a redesign. It is a graft.

IN ONE SENTENCE

This paper is the ecosystem. It extends the graft beyond a single infrastructure to imagine an Internet where every packet carries a readable intent, where platforms are interfaces and not prisons, and where data belongs to you by protocol.

1. The Jellyfish

Imagine an organism without a spine. A jellyfish. It floats. It survives. But it has no central memory, no structured nervous system, no coordinated immune response. If you cut it in two, each half continues to function — but neither learns from the wound. Neither remembers it.

This is the Internet today.

TCP/IP connected the machines. HTTP shared the documents. DNS named the addresses. But no one gave this network a spine. No immune memory. No verifiable identity without a central authority. No data ownership certified by the protocol.

The result is an invertebrate Internet, soft, where:

- YouTube owns your videos, not you.
- Google reads your emails to sell you ads.
- Facebook traps your memories in a walled garden to which you have no key.
- A ransomware thwarted in Paris does not immunize a hospital in Tokyo.
- Your connected device can be drafted into a botnet without your knowledge.

The jellyfish works. But it does not remember. It does not learn. It does not protect. It is not alive.

DIAGNOSIS

The Internet is not sick. It is incomplete. It lacks a fourth pillar — after TCP/IP (communication), HTTP (sharing), and DNS (naming). It lacks immune memory.

2. The Spine

The Symbiotic Internet rests on a simple idea: SPINA as the cryptographic spine.

In a vertebrate network, every packet does not merely carry data. It carries an intent. A cryptographically signed capability manifest that declares: "I am a legitimate request. I come from this node. I can only read, not write. Here is the proof."

The manifest is not a declarative text field. It is a structural proof. A node that claims to "observe" but whose manifest includes a write capability is rejected before the first connection. Intent is readable — not in what the node says, but in what its code allows it to do.

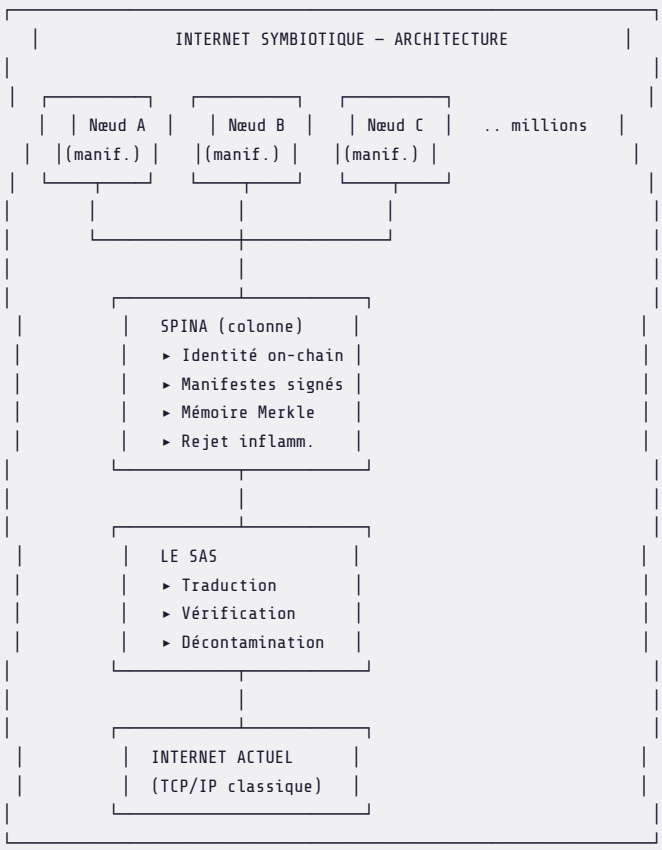

Figure 1: The Symbiotic Internet — SPINA as the spine, the Airlock as the bridge

The spine changes everything. A threat detected by a node in Berlin is recorded in SPINA. In under five minutes, every node on the network — from Tokyo to São Paulo — is immunized. Memory is collective. Defense is distributed. Requisite variety is satisfied (Ashby, 1956).

PRINCIPLE

A threat seen once. Never again anywhere. For anyone. Forever. This is the promise of SPINA. This is the condition of the Symbiotic Internet.

3. You, Not Them

In today's Internet, your identity belongs to Google. Your reputation belongs to Facebook. Your history belongs to Amazon.

In the Symbiotic Internet, you are your own authority. Your identity is a cryptographic key registered in SPINA. Not an email at Gmail. Not an account at Apple. A key that you — and you alone — hold.

When you publish a video, SPINA certifies that you created it. Not YouTube. The platform is merely an interface — a temporary window onto your content. If it shuts down, your content remains. If it abuses, you switch interfaces. Ownership is verified by the protocol, not by the gatekeeper.

DEFINITION – SYMBIOTIC IDENTITY

A symbiotic identity is an Ed25519 keypair registered in SPINA. It is:

▸ Self-sovereign — you hold it, not a third party.

▸ Verifiable — any node can prove it is valid without knowing you.

▸ Portable — it works across all interfaces, all platforms, all services.

▸ Revocable — in case of compromise, a new key is issued, the old one is marked in SPINA.

Spam becomes impossible — not because it is filtered, but because a sender without a verified identity is rejected by the network before ever reaching an inbox. Phishing dies — because an email claiming to come from your bank but whose manifest does not match your bank's on-chain identity is blocked at the protocol level. Not at the user level. At the network level.

4. What Is Yours Stays Yours

The current economic model is simple: platforms offer you a free service in exchange for your data. They store it, analyze it, monetize it. You are not the customer. You are the product.

The Symbiotic Internet reverses this logic. The data belongs to you. The platform is the guest.

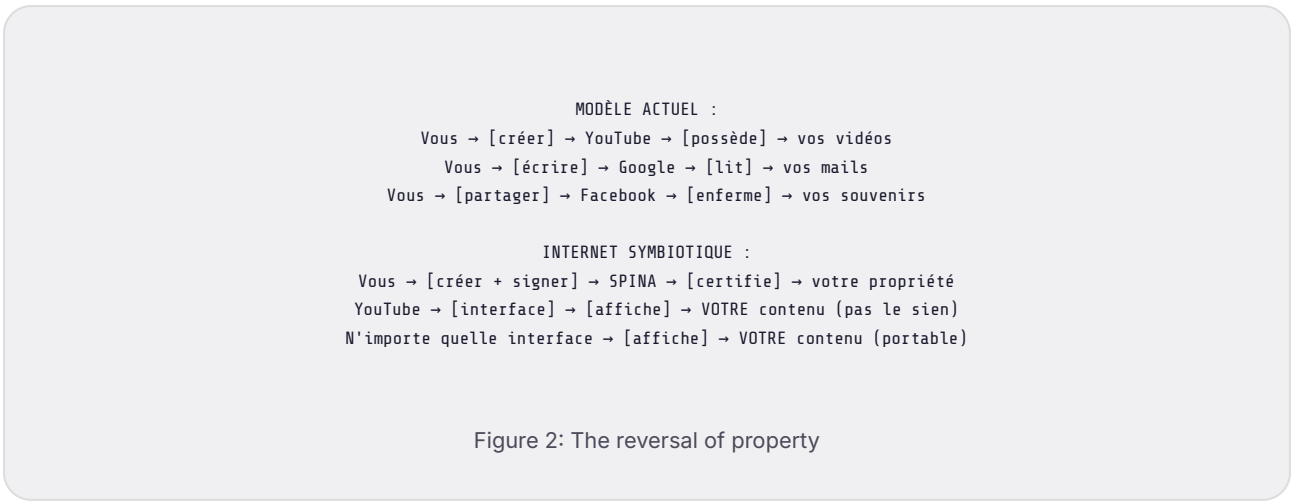

Figure 2: The reversal of property

Decentralized YouTube is not a utopia. It is YouTube where the video, the views, the comments, the revenue — everything is certified to you by SPINA. Anyone can create an interface. The value is in the content — and the content is yours. Verifiable. Portable. Inalienable.

The same principle applies to everything: emails, documents, health records, property titles, diplomas, patents, contracts. Everything that today depends on a trusted third party to exist can be certified by the protocol — without a third party, without fees, without a single point of failure.

REVERSAL

You do not "beat" Google. You make the model obsolete. When ownership is native to the protocol, the gatekeeper has no reason to exist.

5. The Airlock — Coexisting Without Breaking

The Symbiotic Internet does not demand that we sever the old network. That would be an amputation. And NOVA does not migrate — it grafts.

The Airlock is the gateway between the two worlds. It is a SPINA node that inspects incoming traffic from the classical Internet:

1. **Inspection.** Every incoming packet is examined. Does it have a manifest? A valid signature?
2. **Translation.** Classical traffic is encapsulated with a temporary manifest signed by the Airlock — "This packet originates from the non-vertebrate Internet. Limited trust."

3. **Decontamination.** If the packet carries a threat signature known to SPINA, it is rejected before entry. The Airlock is a decontamination airlock — like those in biological laboratories.
4. **Learning.** Malicious patterns detected by the Airlock enrich SPINA. The network learns from its border.

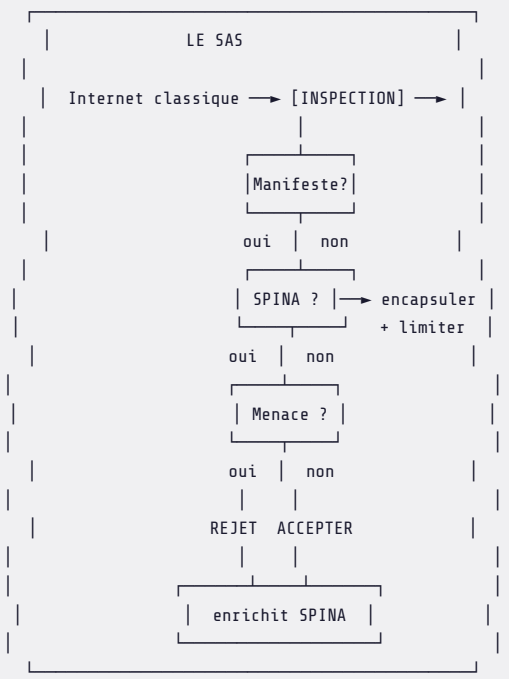

Figure 3: The Airlock — inspection, translation, decontamination

The Airlock enables gradual adoption. A business can deploy the Airlock at the edge of its existing network. Gradually, its internal services migrate to SPINA identities. External traffic continues to pass through the Airlock. There is no D-Day. There is a symbiotic transition.

6. The Promise

The Symbiotic Internet is not a technological innovation. It is the **restoration of a natural state**.

The symbiotic man — the one who lived in harmony with his environment, who did not need to study in order to know — that man has been exiled from his own network. He was dispossessed of his data, his identity, his memory. He was locked into walled gardens while being told it was progress.

The Symbiotic Internet returns to him what is his. Not by adding a layer of protection. By changing the nature of the network — from jellyfish to vertebrate, from amnesiac to immune, from extractive to symbiotic.

Here is the promise, in seven points:

TODAY'S INTERNET	THE SYMBIOTIC INTERNET
Your data belongs to platforms	Your data is certified to you by the protocol
Your identity is an account at Google	Your identity is a key you hold
Spam is filtered (sometimes)	Spam is technically impossible
Phishing relies on your vigilance	Phishing dies at the protocol level
Each threat is fought in silos	Each threat immunizes the entire network
Security is an added layer	Security is an emergent property of the network
You are the product	You are the owner

THE PROMISE

A network where man is no longer the product — but the sovereign. Where every packet carries a readable intent. Where every threat, once seen, can never harm again. Where platforms become windows once more, not prisons.

This is not a new network. It is the network remembering what it should always have been.

References

[1] H. TIKIJJA, "The Law — Unified Foundation of Digital Organisms," 0DATA Lab, Paper 000, 2026.

[2] H. TIKIJJA, "SPINA — The Cryptographic Backbone," 0DATA Lab, Paper 008, 2026.

[3] H. TIKIJJA, "The Immune System of Infrastructures," 0DATA Lab, Paper 005, 2026.

[4] H. TIKIJJA, "The Convergence — The Architecture That Was Waiting for Its Name," 0DATA Lab, Paper 007, 2026.

[5] H. TIKIJJA, "The Digital Graft," 0DATA Lab, Paper 004, 2026.

[6] W.R. Ashby, An Introduction to Cybernetics, Chapman & Hall, 1956.

[7] J. Zittrain, The Future of the Internet — And How to Stop It, Yale University Press, 2008.

[8] J.C. Plantin, C. Lagoze, P.N. Edwards, "Infrastructure studies meet platform studies," New Media & Society, 2016.

[9] J. Benet, "IPFS — Content Addressed, Versioned, P2P File System," arXiv:1407.3561, 2014.

[10] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[11] R.C. Merkle, "A Digital Signature Based on a Conventional Encryption Function," CRYPTO '87, 1987.