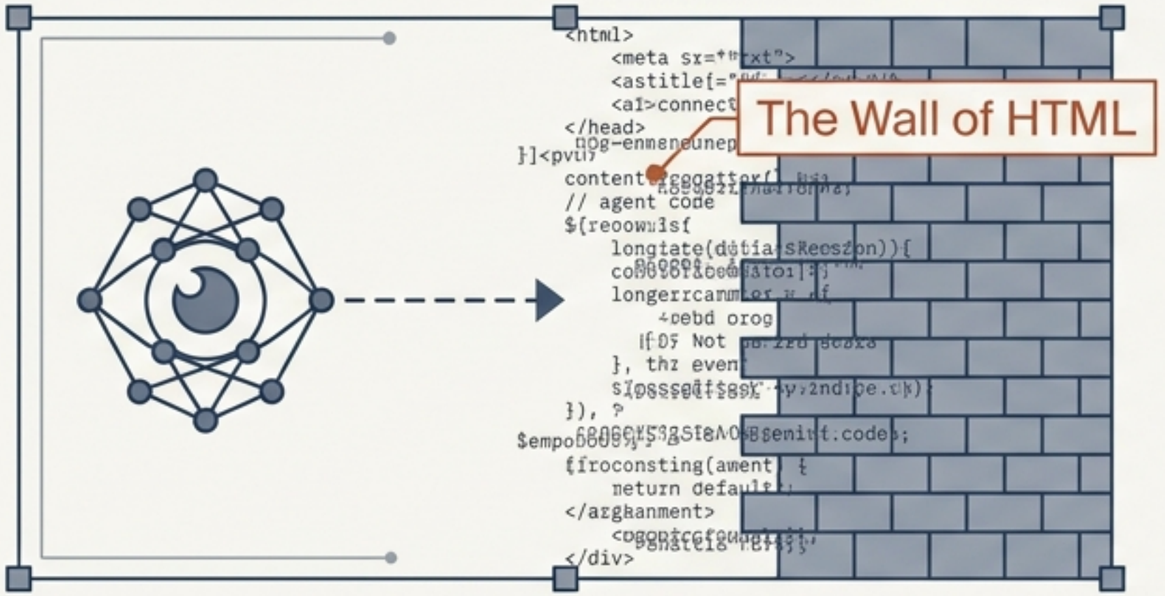
Architecting the Machine-Readable Firm

Moving beyond HTML to build a federated, verifiable knowledge graph for the AI era.

A case study on structuring ægis.no

The invisible AI-era firm.




```
1  contradiction: true
```

An AI-era consulting company that isn't machine-readable is a contradiction.

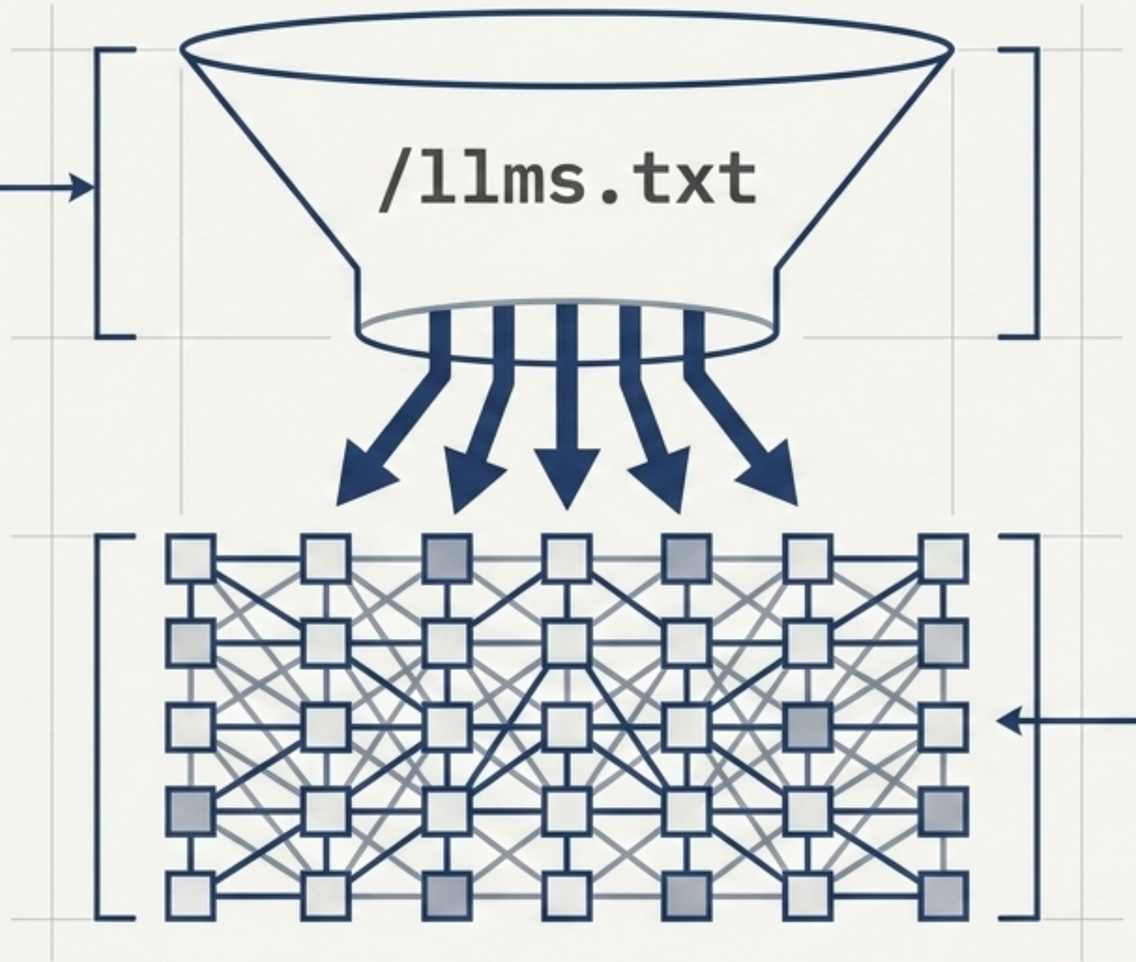
```
1  evaluation_pipeline: failed
```

Clients will use AI to evaluate you. Agents look up your services, methodology, and pricing model. If the only thing they find is HTML, you are invisible to half the evaluation pipeline before the first conversation even starts.

The Two-Tier Architecture

The Gateway (Simple)

Simple markdown routing via /llms.txt.



The Protocol (Advanced)

Structured, federated, and signed YAML capability graph via KCP.

KCP (Knowledge Context Protocol)

The bare minimum: `/llms.txt`

/llms.txt

```
# ægis.no Capabilities

We offer specialized AI consulting.

## Services

- Advisory
- Workshops

## Context

Find detailed structured data at /knowledge.yaml
```

The llmstxt.org spec is refreshingly simple.

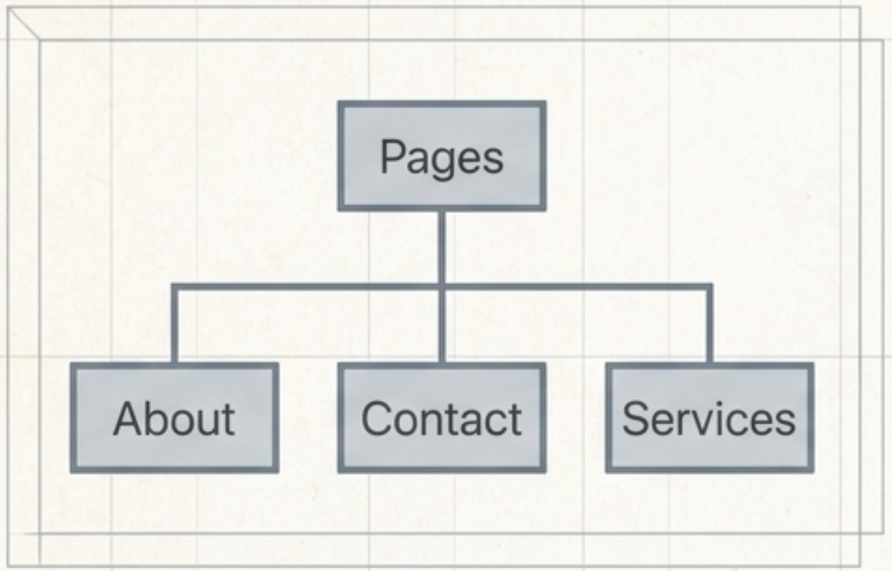
One Markdown file describing your site for language models: what you offer, where to find things, what context matters.

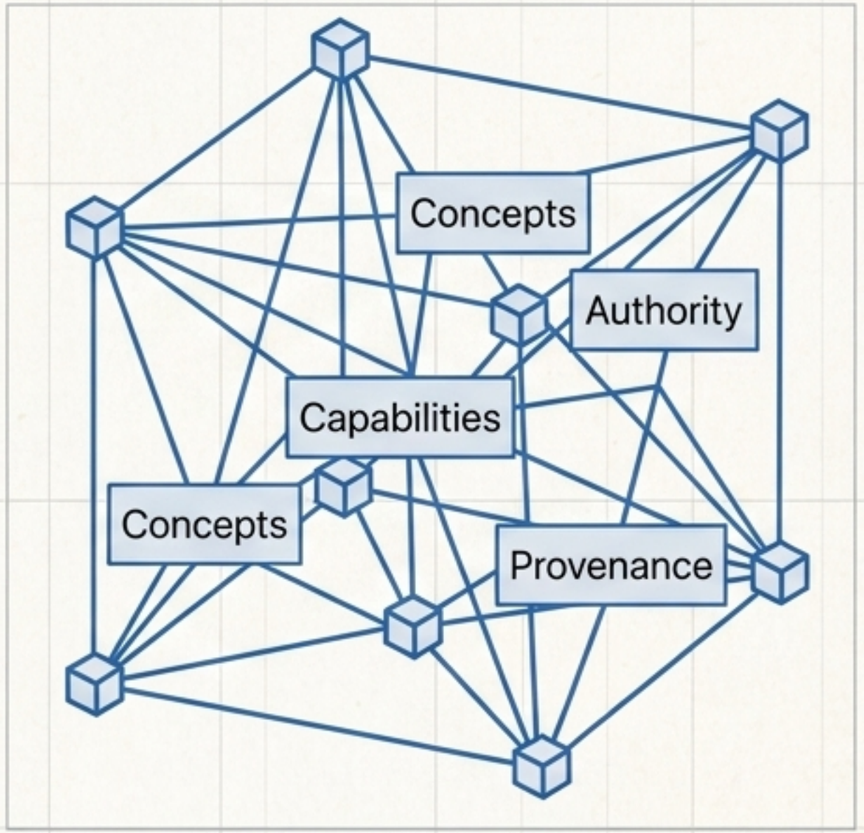
5 minutes of writing + 5 minutes of deployment.

The ROI Box

Any agent querying your site gets a clean starting point instead of being forced to reverse-engineer your navigation structure.

Transitioning to the Knowledge Context Protocol (KCP)



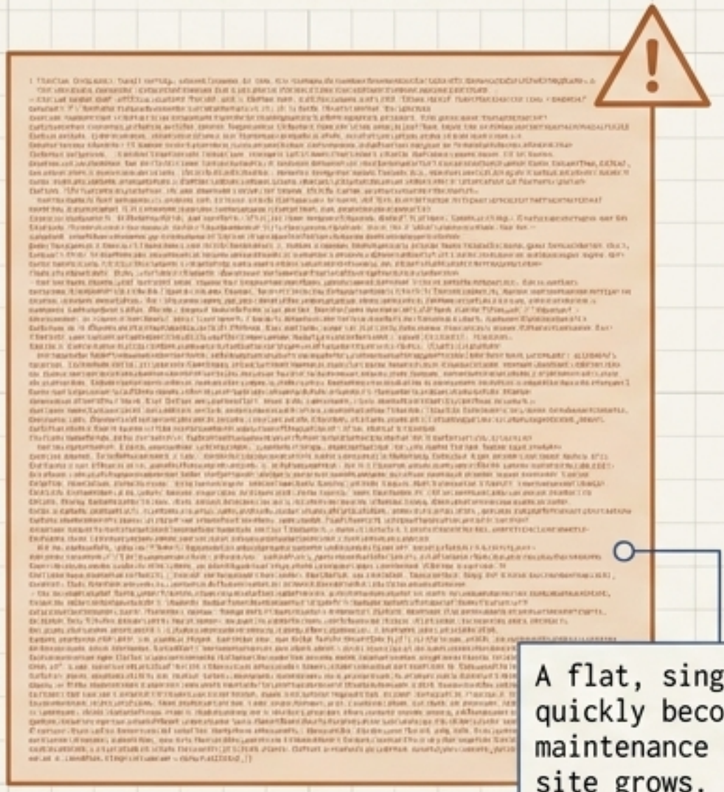


KCP is a YAML-based protocol for publishing structured knowledge as a machine-readable graph.

Think of it as a sitemap, but for concepts and capabilities rather than pages—with authority, provenance, and cryptographic signing natively baked in.

The design rationale for federation.

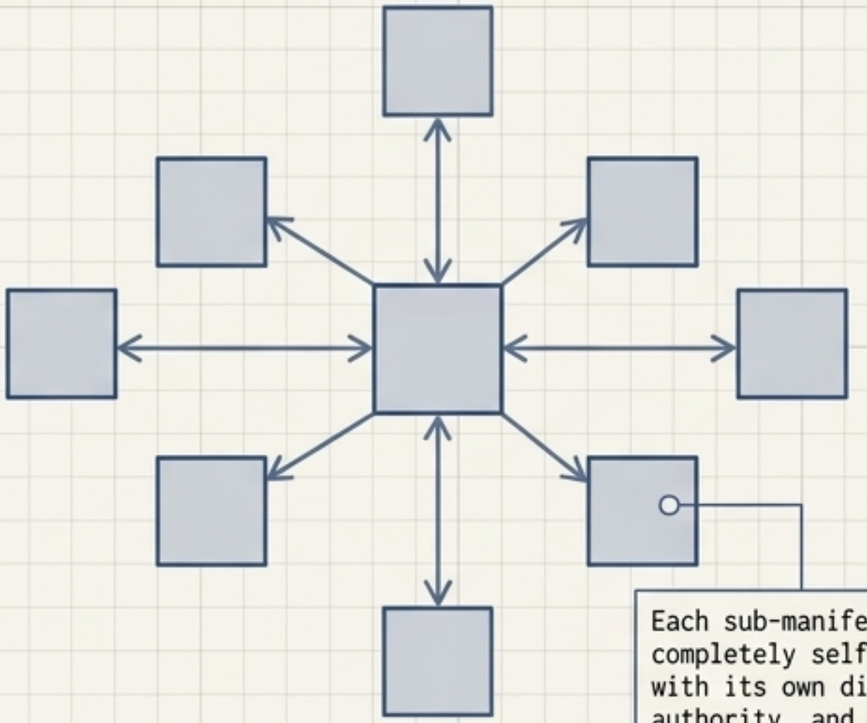
The Anti-Pattern



A flat, single manifest quickly becomes maintenance hell as a site grows.

Flat YAML

The Solution

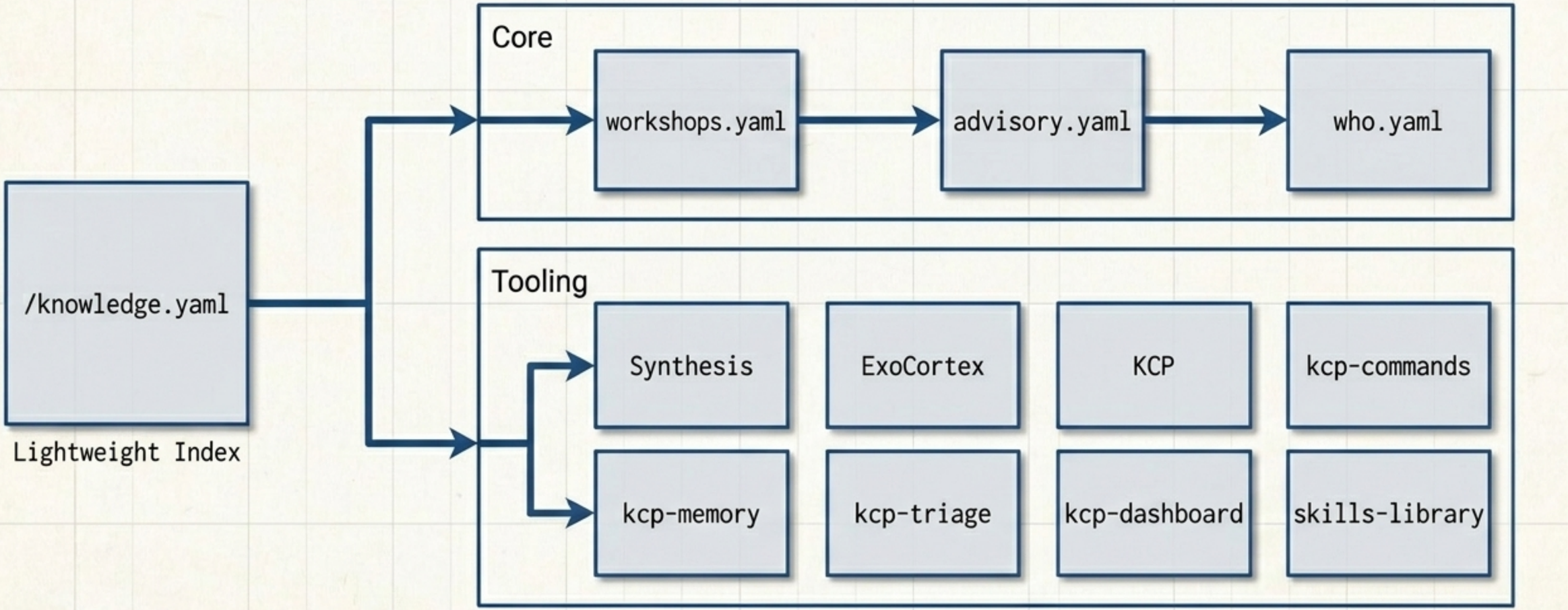


Each sub-manifest must be completely self-contained with its own discovery, authority, and signing blocks

Federated Architecture

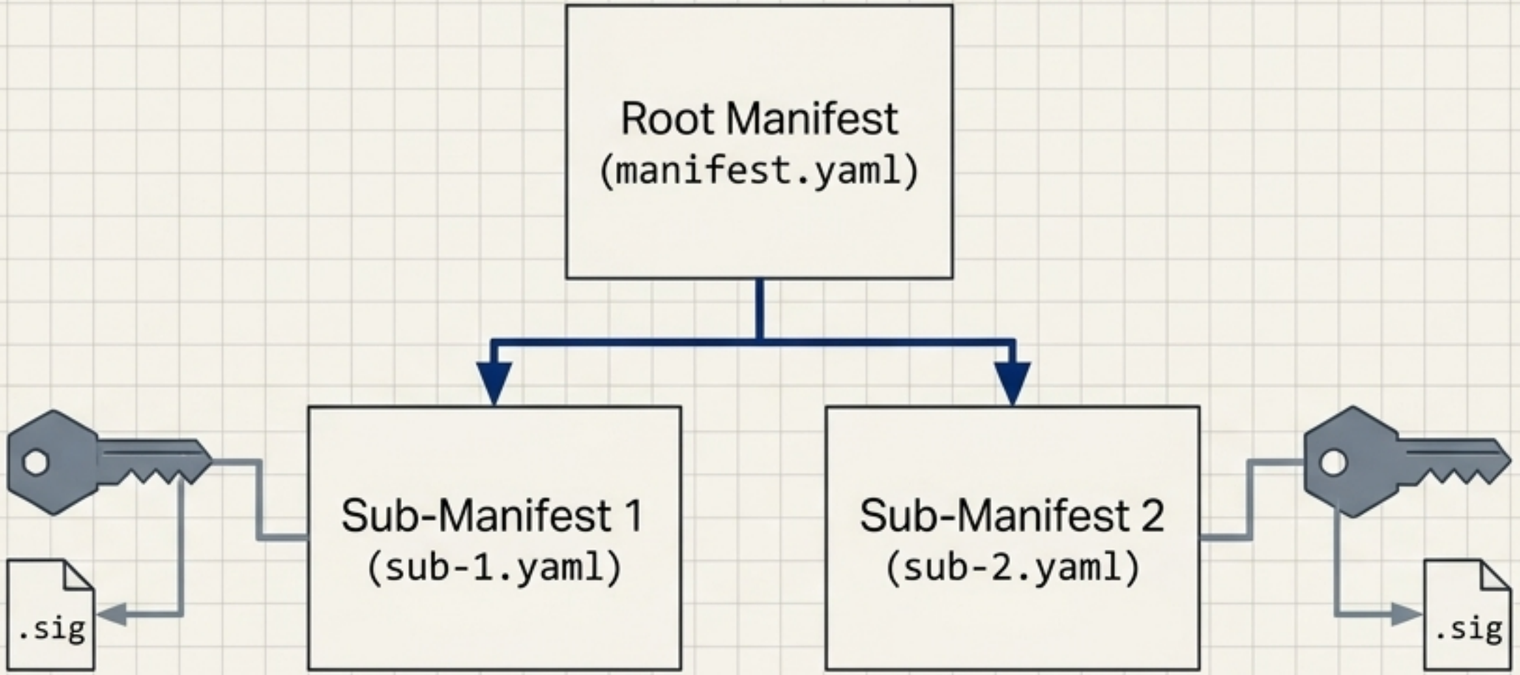
Federation keeps each domain of knowledge exclusively owned by the people who actually understand it.

Mapping the ægis.no capability graph.



Solid lines represent federation links. Each distinct node represents an independently manageable YAML manifest.

Verifiable Provenance via Option A Signing.

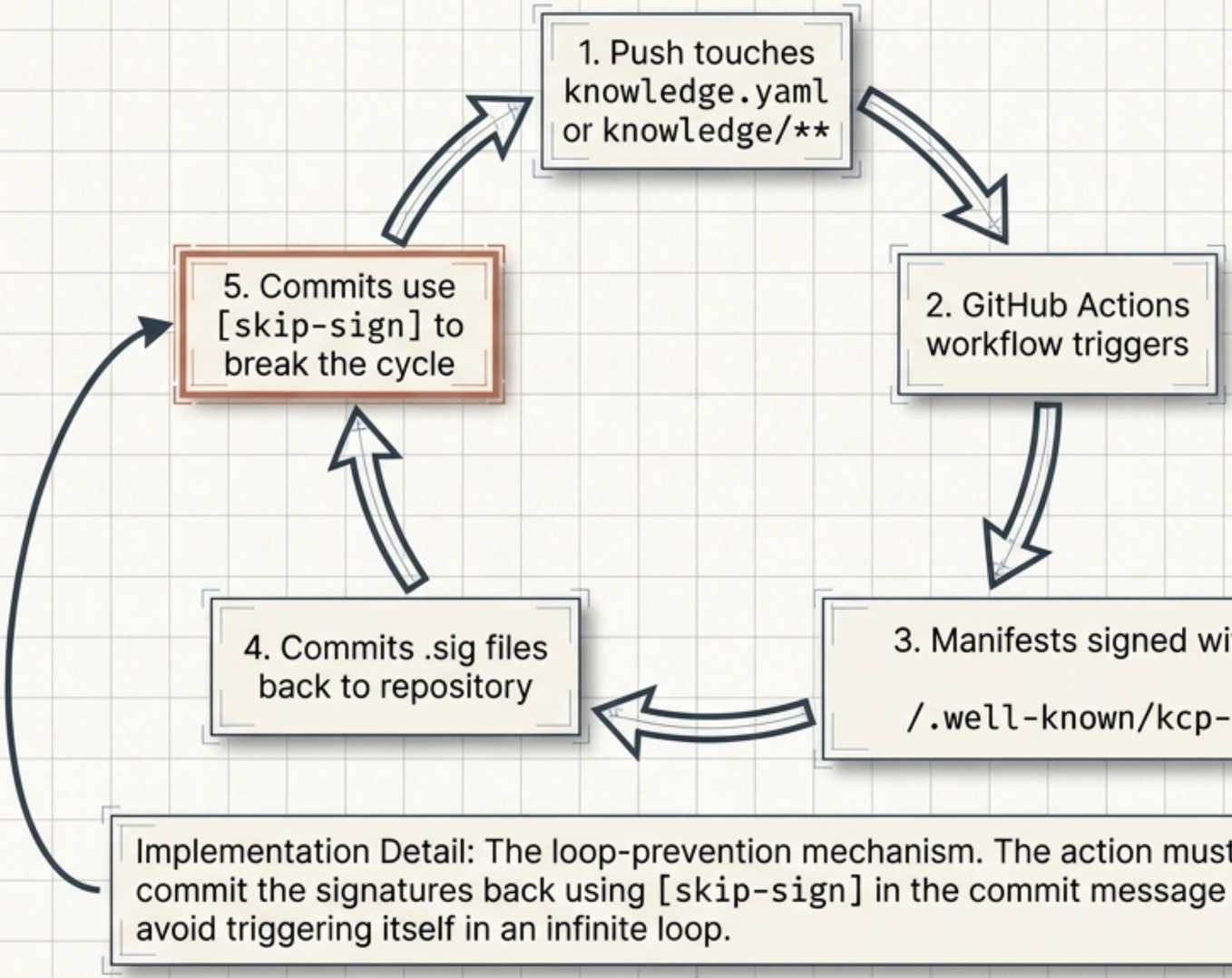


KCP supports multiple models. Option A means each sub-manifest is independently signed.

Different manifests can be signed by different keys. A partner contributing a sub-manifest can sign it with their own key, anchoring provenance directly to the author.

The Golden Rule of Trust: Canonical data in a KCP manifest is merely self-asserted unless you sign it. Signing makes the graph verifiable.

The automated signing pipeline.



Currently, all 11 ægis.no manifests are signed by a single GitHub Actions

GitHub Actions workflow key.

Implementation Detail: The loop-prevention mechanism. The action must commit the signatures back using [skip-sign] in the commit message to avoid triggering itself in an infinite loop.

The Ed25519 Cryptography Gotcha

```
Error: operation not supported
for this keytype
```

```
Fix: openssl pkeyutl -rawin ...
```

The Issue:

Ed25519 doesn't use an external digest algorithm; the hash is internal, meaning you must sign the raw bytes directly.

The Cause:

By default, openssl pkeyutl tries to perform a separate hashing step that Ed25519 simply does not support, causing the pipeline to fail.

The Fix:

Explicitly pass the **-rawin** flag to sign the raw bytes.

Architectural Paradigm Shift

Traditional Web Firm	Machine-Readable Firm
HTML & CSS	**Markdown & Structured YAML**
Designed for Human Parsing	**Designed for AI Agent Ingestion**
Flat Page Hierarchy	**Federated Capability Graph**
Implicit (Brand Design)	**Cryptographically Verifiable Provenance**

From Storefront to Verified API.

Being AI-ready is not about SEO. By combining the immediate discoverability of /llms.txt with the federated, cryptographically signed structure of KCP, you transform your firm.

Your firm’s capabilities stop being static marketing text and become **natively executable protocols** for the agents evaluating you.