



SOLARA ASSOCIATES

# UAB × SYNTHERA

Compose governed multi-agent systems. **Pick any protocols.**  
SYNTHERA runs underneath — every agent identified,  
bounded, and its delegation contained. Identity and least-  
privilege delegation are enforced live on Cloud Run.

Go-to-market deck   Version 1.0   6 July 2026   solara.associates

THE LAYER NOBODY OWNS YET

# Agent identity is solved. Agent delegation is not.

## IDENTITY — HANDLED

The industry standardised cryptographic workload identity on SPIFFE. Everyone agreed agents need identity, and the standard is set. This is table stakes now.

## DELEGATION — UNGOVERNED

But identity is not containment. Agents spawn agents — and nothing stops a sub-agent from exceeding the authority its parent had. The floor governs what an agent is, not what it may delegate.

## FAIL-OPEN IS CATASTROPHIC

In a multi-agent system, a delegation that defaults to “allow” isn’t a bug — it’s a breach waiting to propagate down the tree.

Identity says **who** an agent is. Nobody yet owns the layer that governs **what it may delegate**.



## THE INSIGHT

# Identity says who an agent is. SYNTHERA governs what it may delegate.

### WHAT THE BUILDER PICKS — THE AGENT'S SURFACE

MCP

A2A

ADK

AP2

LangChain

OpenAI Agents

Free · volatile · swappable — the primary surface the builder controls.

### WHAT SYNTHERA GUARANTEES — AUTOMATIC, NON-OPTIONAL

Identity

Lineage

Attenuated scope

Containment

Every agent gets a cryptographic identity, a place in the delegation tree, a bounded scope, and foundation-enforced containment — no matter which protocols it speaks.



WHAT “GOVERNED” MEANS, CONCRETELY

# Four primitives, enforced at the foundation — not in the app

## IDENTITY

Every agent is minted a verifiable cryptographic identity (VAID). It can never act anonymously.

## LINEAGE

Delegation is a single-parent tree. Who spawned whom is provable and recorded.

## ATTENUATION

A child's authority is always a subset of its parent's. Power only narrows downward.

## CONTAINMENT

An over-scope spawn is denied by the foundation — fail-closed, even if the app is bypassed.

The builder never wires any of this. It happens to every agent, on provision.



## THE PRODUCT

# Compose a system. Watch it provision. Trust runs underneath.

1

### Compose roles

Drag in agent roles. Pick the protocols each one speaks — freely, the primary surface.

2

### Draw delegation

Define who may spawn whom. Scopes auto-template; you see the bounds without filling a form.

3

### Provision

One click mints the governed identities and deploys the root on the live foundation.

4

### See it enforced

Watch SYNTHERA mint, delegate — and deny an over-scope spawn, live.

| Protocols are what the agent speaks. SYNTHERA is what it is — and what it's allowed to be.



PROOF 1 OF 2 – LIVE, NOT A MOCK

# Change the protocols. Governance doesn't move.

The orthogonality is the moat — proven as a passing test in the product, and visible on screen.

VOLATILE – PROTOCOLS (CHANGE FREELY)

|           |   |     |
|-----------|---|-----|
| MCP       | → | A2A |
| REST      | → | AP2 |
| LangChain | → | ADK |

INVARIANT – SYNTHERA GOVERNANCE

|                              |              |             |
|------------------------------|--------------|-------------|
| identity                     | ec3f83e1...  | ✓ unchanged |
| scope                        | demo/safe/   | ✓ unchanged |
| lineage                      | root → child | ✓ unchanged |
| governanceDiff = [ ] – empty |              |             |

Protocols moved; governance didn't. That is SYNTHERA under everything.

# Try to escape the envelope. The foundation refuses.

Not a UI check. A deployed agent attempts an over-scope delegation; the live foundation denies it — fail-closed.

```
// illustrative – real path: POST /tools/call (mint_child), probed via /probe/over-envelope
POST /tools/call · mint_child      → the live foundation (Cloud Run)
  parentScope: [ "demo/safe/" ]    // the authority granted
  childScope:  [ "demo/secret/" ]  // attempts to exceed it

→ denied: true   (HTTP 200, foundation verdict)
"child scope exceeds the parent's – least-privilege attenuation denied"
```

The foundation's own verdict, returned over HTTPS from the live deployment — enforced in the foundation, not the UI. **The moat is real, not UI-deep.**



HOW IT FITS TOGETHER

# One foundation. Many surfaces. Frameworks are adapters, not rebuilds.

## THE BUILDER

### UAB

Public, self-serve. Compose roles, pick protocols, provision. The product.

→

## THE ADAPTERS

### Framework adapters

LangChain in automated CI; ADK and OpenAI implemented with test suites and a live demo harness, automated coverage in progress. The pattern generalises to any framework.

→

## THE FOUNDATION

### SYNTHERA

Identity, lineage, attenuation, containment. The constant beneath every surface — the moat.

Adding a framework touches one adapter — **never the foundation, the spec, or the governance.** The moat is the constant.



STRAIGHT ABOUT WHERE IT STANDS

# What's live today — and what's deliberately next

## LIVE & PROVEN

- ✓ Compose governed multi-agent systems in the browser
- ✓ Per-role protocol surface, fully configurable
- ✓ Operator-mediated mint · bring-your-own-key · per-call proof-of-possession
- ✓ Attenuated delegation, foundation-enforced (fail-closed)
- ✓ LangChain integration implemented and covered by automated CI
- ✓ End-to-end on Cloud Run — browser → live foundation (identity & delegation)

## DELIBERATELY NEXT

- Per-user sovereign key custody
- Self-serve onboarding at scale
- Action-level policy (today: identity & scope governance)
- Durable audit & revocation of record
- ADK & OpenAI adapters implemented — automated CI coverage in progress

Every “next” is scoped and gated — **nothing here is hand-waved.**



WHY THIS WINS

# The unowned layer, above identity and across everything

## THE LAYER ABOVE IDENTITY

### Delegation, not just identity

The identity floor governs what an agent *is* and what it can touch. SYNTHERA governs what an agent may *delegate* — a child's authority cryptographically bounded by its parent's. It sits above the identity layer the industry standardised, not against it.

## DOUBLE NEUTRALITY

### Framework- and cloud-agnostic

A first-party stack is locked to one framework and one cloud — its funnel won't let it be neutral. The delegation-governance layer is unowned and cross-everything. That intersection is the defensible ground.

Land the standard before the platforms notice it's a layer worth owning. **Neutral, cryptographic, portable** — the layer no incumbent is built to hold.



SEE IT WORK

# See SYNTHERA work.

Pick any protocols. Compose a governed system. Watch the foundation **mint it, bound it, and deny what exceeds it** — live in your browser.

Live demo `solara.associates`    Talk to us `info@solara.associates`

