

AGENT ACCESS LAYER

Agents can act. Can we trust them?

Scoped authority and verifiable human control for agentic actions.

The interface changed. The trust model didn't.

01 Intent is not authority

A prompt explains what someone wants—not what an agent is permitted to do.

02 Access is too coarse

Traditional scopes rarely express tools, limits, payment boundaries, and revocation together.

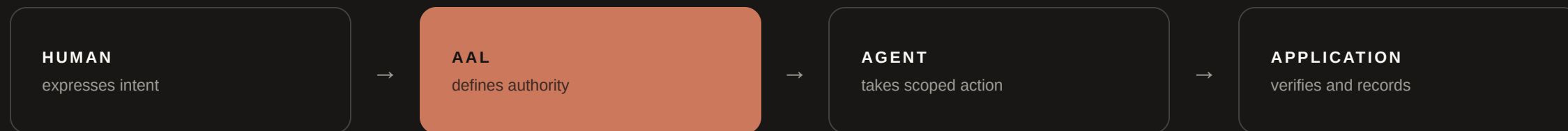
03 Logs arrive too late

Post-hoc records cannot prove that authority was enforced when an action occurred.

04 Attribution disappears

Agent choices and human changes collapse into the same application state.

AAL is the missing trust layer.



Explicit.

Machine-readable Grants define tools, limits, and boundaries.

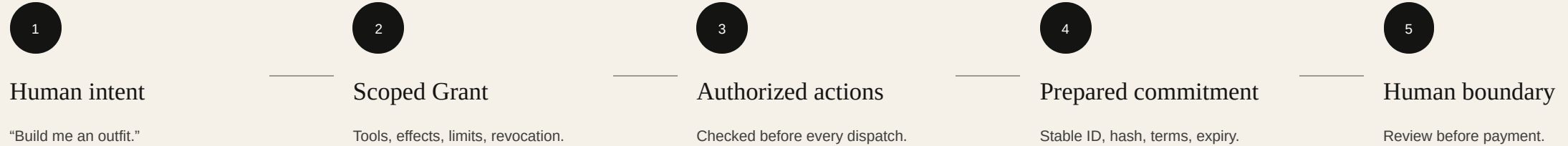
Enforceable.

Every consequential call is checked before dispatch.

Provable.

Agent, protocol, and human actions remain attributable.

One Grant. Every consequential step.



THE CRITICAL DESIGN CHOICE

Preparation is not execution.

The agent can assemble a consequential action without automatically crossing its final boundary.

LIVE DEMO

Make it concrete.

Northline Outfitters is a fictional fashion store built on the real AAL protocol services.

28

CATALOG PRODUCTS

3

GRANTED TOOLS

0

PAYMENT AUTHORITY

USER REQUEST

“I need an outfit with blue jeans and a cropped boxy white t shirt.”

STYLE MY OUTFIT →

THE RESULT

From request to prepared outfit.

Five coordinated products selected

Every choice attributed to the agent

\$256 transaction prepared from exact records

Commitment ID, hash, terms, and expiry

YOUR EDIT

The outfit, assembled.

AAL CORE GRANT ACTIVE



TOPAGENT

Essential Boxy Crop Tee

White · \$34.00

Matched white, cropped, crop.

REMOVE



BOTTOMAGENT

Vintage Straight Jean

Medium wash · \$78.00

Matched blue, jeans.

REMOVE



SOCKSAGENT

Cloud Rib Crew Socks

Cream · \$14.00

Matched white.

REMOVE



HATAGENT

Washed Twill Cap

Navy · \$32.00

Matched blue.

REMOVE



SHOESAGENT

Minimal Court Sneaker

White · \$98.00

Matched white.

REMOVE

PREPARED TRANSACTION

Total

\$256.00

Essential Boxy Crop Tee	\$34.00
Vintage Straight Jean	\$78.00
Cloud Rib Crew Socks	\$14.00
Washed Twill Cap	\$32.00
Minimal Court Sneaker	\$98.00

WHAT HAPPENED

5 EVENTS

COPY AUDIT JSON

Open any event to see its plain-language meaning and sanitized protocol metadata.

✓

AAL session established

Authenticated demo session is bound to this storefront.

AAL

▼

✓

Core Grant installed

Consent approved for 3 tools · payer none.

AAL

▲

WHAT HAPPENED

The stylist received a revocable, non-payment Grant covering catalog searches, product reads, and transaction preparation.

Not a post-hoc story. An enforced history.

01	AAL session established	AAL
02	Core Grant installed	AAL
03	Catalog explored	AGENT
04	Outfit composed	AGENT
05	Transaction prepared	AGENT

CATALOG PHASE METADATA

5

categories searched

24

records considered

5

records read

allowed

authorization

true

AAL Grant used

THE BOUNDARY

The thing the agent *cannot* do matters most.

grant.payer	none
payment_permission	false
transaction.state	prepared
payment.status	not_started

The limitation appears in the Grant, authorization evidence, transaction state, and interface.

Fashion makes it visible. The protocol goes everywhere.



Travel

Search itineraries and prepare a booking before purchase.



Procurement

Build a purchase order inside policy and budget limits.



Healthcare

Scope access to sensitive records and approved purposes.



Financial services

Research and prepare a trade before final authorization.

WHAT'S NEXT

From complete demonstration to agent infrastructure.

NOW

Proven trust loop

Grant Consent and Host Evidence

Lifecycle and dispatch enforcement

Attributable agent/human actions

Prepared commitments and audit export

NEXT

Production integration

External agent runtime adapters

User-managed Grants and revocation

Trusted approval displays

SDKs and conformance tooling

THEN

Consequential execution

Payment behind explicit approval

Travel and procurement profiles

Portable cross-site receipts

Interoperable agent ecosystem

Agents need more than intelligence.

They need accountable authority.

AAL makes agent authority **explicit**, **enforceable**, and **provable**.