



Agentic AI Foundation

# AGNTCon + MCPCon North America

Where the **agentic stack** is being built.

## Interoperable Agent Discovery

AI Catalog, ARD, and the AGNTCY Directory

**Junjie Bu**

Senior Staff Engineer, Google

ARD co-author, AI Catalog TSC

**Luca Muscariello**

Distinguished Engineer, Cisco

AGNTCY TSC, A2A TSC, AI Catalog maintainer

# How agent tools are found today

## FIND

### Per type

a separate directory for each kind of resource

Skills: skills.sh, ClawHub  
MCP: MCP Registry, Smithery, Glama  
A2A: A2A Registry, cloud registries  
Plugins: a store in each client

## INSTALL

### Per client

copy a config or run a CLI, for every tool

```
npx skills add <repo>  
edit mcp.json  
/plugin install <name>
```

## TRUST

# 13.4%

of 3,984 scanned skills had critical issues

76 confirmed malicious (Snyk, Feb 2026). Scan results stay in each tool and aren't tied to the version you install.

Finding, installing, and trusting are all manual today.

Where the **agentic stack** is being built.

# Agentic resources keep growing

An agentic resource is **anything** an agent can use to get a task done.

## MCP server

`.../mcp-server-card+json`

## A2A agent

`.../a2a-agent-card+json`

## Agent skill

`.../agent-skills+md`

## Plugin

`.../agent-plugins+zip`

## Knowledge (OKF)

`text/vnd.okf+markdown`

## API

OpenAPI · GraphQL

## Dataset · model

`.../parquet` · model card

## Catalog of catalogs

`.../ai-catalog+json`

Each has its own format, and new ones keep arriving.

Where the **agentic stack** is being built.

# What an entry looks like

```
{  
  "identifier": "urn:air:example.com:skill:code-review",  
  "type": "application/agent-skills+zip",  
  "url":  
    "https://skills.example.com/code-review/skill.zip",  
  "representativeQueries": [  
    "review this change before I share it"  
  ]  
}
```

NAME **identifier**

Unique, includes the publisher's domain

TYPE **type**

What it is, so the client knows how to use it

LOCATION **url or data**

The resource in its own format, or inline

FINDABLE **representativeQueries**

What search services rank on (ARD)

Only the type changes:

MCP server

A2A agent

Skill

The same fields describe every kind of agentic resource.

Where the **agentic stack** is being built.

# Identify, then verify

## trustManifest

### identity

did:web:example.com who signs

### subject

identifier + digest exactly which artifact

### attestations[ ]

type · uri · digest evidence, by scope

### signature

detached JWS covers all of it

## Compliance

SOC2-Type2 · HIPAA-Audit

## Security scan

SARIF report of the artifact

## Provenance

SLSA · in-toto DSSE · SBOM

## Transparency log

SCITT receipt · ANS registration

## Runtime evaluation

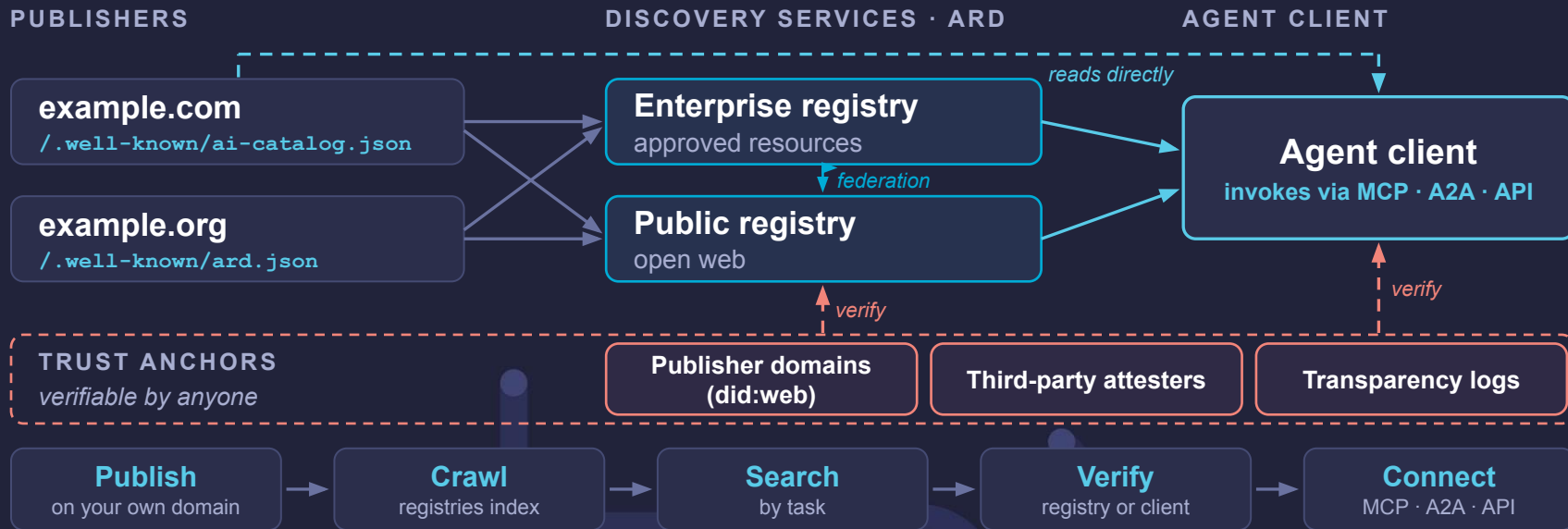
e.g. agent-readiness scorecard

**The data model doesn't run these checks.**

It gives publishers and third parties one place to attach verifiable claims.

Where the **agentic stack** is being built.

# How it fits together



# How a client uses it

```
POST /api/v1/search
Host: agentfinder.github.com
{
  "query": {"text":
    "review a code change before I share it"}
}
```

Same request, any ARD service:

GitHub Agent Finder

Hugging Face Discover

Ora Directory

ANS Finder

**results** ranked by relevance

**Code Review**

`urn:air:github.com:flutter:skills:code-review`

95

**Review Uncommitted**

`urn:air:github.com:smarterabai:agent-skills:review-uncommitted`

90

**Code Review**

`urn:air:github.com:getsentry:skills:code-review`

90

*Live query to GitHub Agent Finder · Oct 18, 2026*

The relevance score is not a trust rating.

Where the agentic stack is being built.

# Who's building it

## ARD · CO-DEVELOPED BY 12 COMPANIES

|         |            |              |           |
|---------|------------|--------------|-----------|
| AWS     | Cisco      | Databricks   | GitHub    |
| GoDaddy | Google     | Hugging Face | Microsoft |
| NVIDIA  | Salesforce | ServiceNow   | Snowflake |

## AI CATALOG

|           |           |          |
|-----------|-----------|----------|
| Anthropic | AWS       | Cisco    |
| Google    | Microsoft | PulseMCP |

*A joint effort of the MCP and A2A communities*

### Search services

GitHub Agent Finder · Hugging Face Discover  
Cisco AGNTCY Directory · Ora · Desvela  
Salesforce Agentforce (building)

### Catalogs in use

Cloudflare · Weaviate · tldraw · Nylas  
Percona · MIT NANDA Index  
and 19 more published catalogs

*Separate specs, compatible entries*

**Next: Luca demonstrates the AGNTCY Agent Directory.**

Where the **agentic stack** is being built.

# AGNTCY Agent Directory demonstration for A2A discovery

## Stored in Directory

The AI Catalog is stored in an OCI storage service.

Directory provides content management services and also artifact storage.

Search API are served via ARD spec.

## Published on the internet

A component catalog to build new agents. For humans and agents.

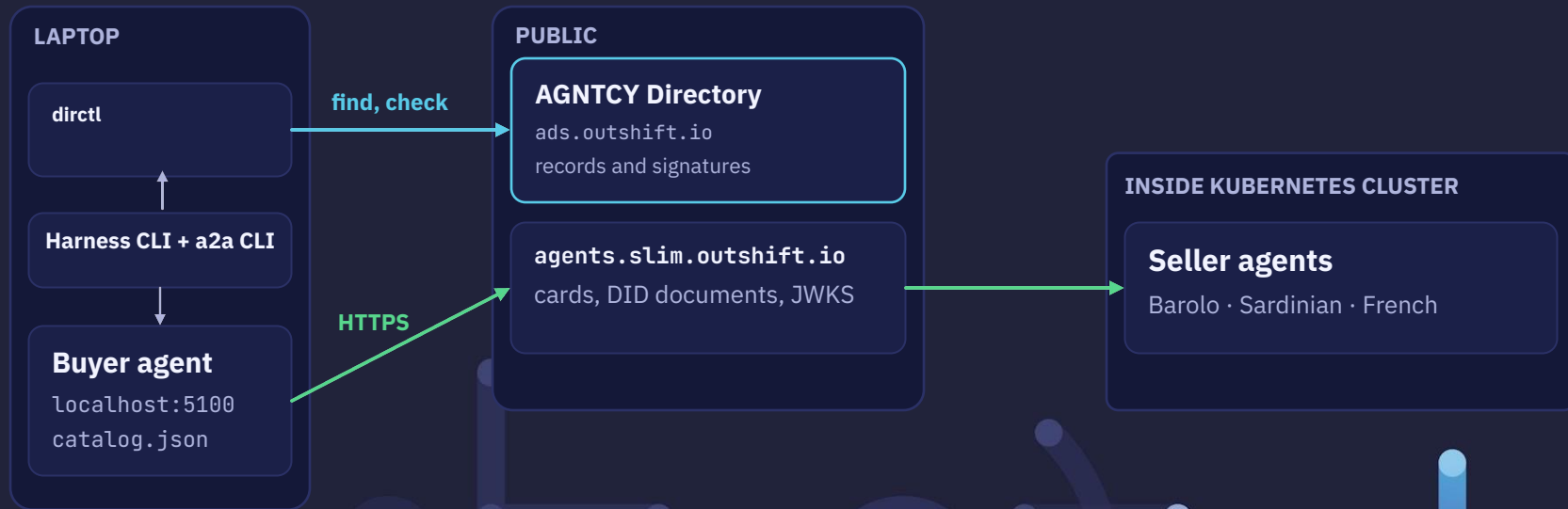
A RDV point for agents to discover other agents.

Where the **agentic stack** is being built.

An abstract graphic at the bottom of the slide consisting of various colored lines (blue, purple, orange, pink) and dots of different sizes, creating a network-like or circuit-like pattern.

# Where everything runs

## THE DEMO TOPOLOGY



Where the **agentic stack** is being built.



## Explore

Browse the secure directory of verified providers

## SEARCH

Filter by name...

## MEDIA TYPE

- ☒ A2A Agent
- ☐ MCP Server
- ☐ SKILL
- ☐ Markdown
- ☐ Bundle

## STATUS

- ☒ Trusted
- ☐ Safe

## TAGS

Filter tags...

Suggest tags

- ☐ Academic Writing
- ☐ Accounting
- ☐ Actuarial Science
- ☐ Ad Copywriting
- ☐ Ad Creative Production
- ☐ Advertising
- ☐ Advertising

<https://agents.slim.outshift.io/agentcon/barolo-supplier>

urn:ai:org.agntcy:cid:baeareicwyjiylqv2jgxu2m3h53gk73nswbscsmimfcwvtr7rc66vez3y6q

<https://agents.slim.outshift.io/agentcon/barolo-supplier> 0.1.1 A2A [Download JSON](#)

## Tags

- oasf:1.0.0:domains:retail\_and\_ecommerce/inventory\_management
- oasf:1.0.0:domains:retail\_and\_ecommerce/online\_retail
- oasf:1.0.0:domains:retail\_and\_ecommerce/order\_fulfillment
- oasf:1.0.0:skills:natural\_language\_processing/natural\_language\_generation
- oasf:1.0.0:skills:natural\_language\_processing/natural\_language\_understanding
- oasf:1.0.0:skills:tool\_interaction/api\_schema\_understanding
- agntcy.dir/identity=did:web:agents.slim.outshift.io:agentcon:barolo-supplier

## Scanner Details

A2a Scanner

Safe · None severity 10/19/2026

## Catalog Entry JSON

[Copy](#)

```
"trustManifest": {
  "identity": "urn:ai:org.agntcy:cid:baeareicwyjiylqv2jgxu2m3h53gk73nswbscsmimfcwvtr7rc66vez3y6q",
  "identityType": "did",
  "attestations": [
    {
      "type": "publisher-identity",
      "uri": "data:application/octet-stream;base64,MEQCICn+DoeQH+GRe2ZMIdkYPJfrFcsZe",
      "mediaType": "application/octet-stream",
      "digest": "sha256:a00c63c50c5218e6647a4e7da4ba097923809d7cfa6238067487ba980a62",
      "size": "70",
      "description": "Verified signature by urn:ai:org.agntcy:signer:key:ECDSA-P-256"
    }
  ]
}
```

<https://agents.slim.outshift.io/agentcon/barolo-supplier>

version 0.1.1 • 10/19/2026

agentCon demo wine seller of Sardinian  
wines (Vermentino di Gallura, Cannon...[Inventory Management](#) [Online Retail](#)  
[Order Fulfillment](#)

A2A

↓ 33 ⓘ 1

<https://agents.slim.outshift.io/agentcon/barolo-supplier>

version 0.1.0 • 10/19/2026

agentCon demo wine seller of French  
wines (Château Margaux, Dom Ruinart...[Inventory Management](#) [Online Retail](#)  
[Order Fulfillment](#)

A2A

↓ 24 ⓘ 1

# A buyer agent buys wine

THE DEMO STORY



Agentic AI Foundation

AGNTCon + MCPCon

North America

This deck

## Search

Look up the wine sellers in the Directory

This deck

## Verify

Who published each record? Which identity does each seller have?

Rest of the demo

## Ask

A quote from every seller, over A2A on SLIM or HTTPS

Rest of the demo

## Buy

The Barolo, after an over-21 proof from a phone wallet

Where the **agentic stack** is being built.

# Three sellers, found by identifier

SEARCH



Agentic AI Foundation

AGNTCon + MCPCon  
North America

## Barolo

agentcon/barolo-supplier

version 0.1.1

baeareicwy...ez3y6q

## Sardinian

agentcon/sardinian-supplier

version 0.1.1

baeareigd7...ye4vyq

## French

agentcon/french-supplier

version 0.1.1

baeareie37...hsqokm

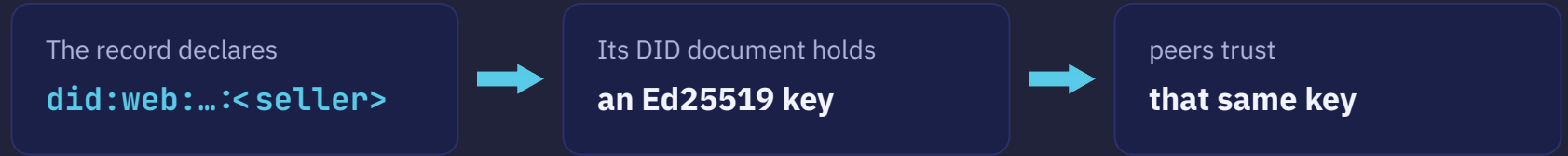
```
$ directl search --name 'https://agents.slim.outshift.io/agentcon/*'
```

Each record carries the seller's A2A card

Where the **agentic stack** is being built.

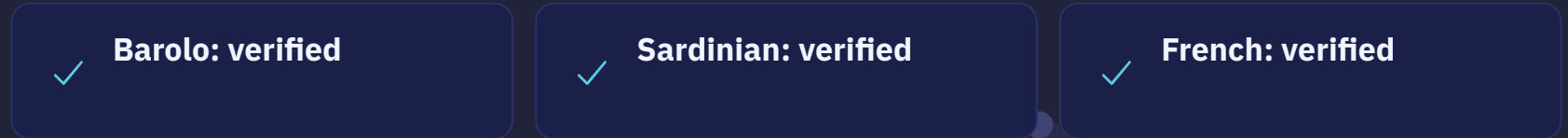
# Each sellers' publisher identity

VERIFY



DIRECTORY IDENTITY CLAIM

`$ directl identity status <cid>`



Where the **agentic stack** is being built.

# Different attestations

## BUILDER OF THE AGENT

### Agent builder

Key: e.g. Microsoft cosign key

```
$ directl push seller-record.json  
$ directl sign <cid> --key  
agentcon-cosign.key --password-stdin
```

Evidence: the signature and the cosign key

## THE RUNNING AGENT'S OWN IDENTITY VERIFICATION

### Each seller

Key: the seller's own Ed25519 key from did.json

```
$ directl identity claim --record <cid>  
--role identity --key seller.pem
```

Evidence: the identity claim, checked against the DID document

# Q&A

- <https://ai-catalog.io>
- <https://dir.agntcy.org>
- <https://agenticresourcediscovery.org>

Where the **agentic stack** is being built.

A decorative graphic at the bottom of the slide consisting of various colored dots (orange, purple, blue, pink) and lines of different colors (purple, blue, pink) arranged in a complex, abstract pattern.