Agent Name Service (ANS): A Universal Directory for Secure AI Agent Discovery

- The Agent Name Service (ANS) is the DNS for agent discovery
  - Protocol-Agnostic Design
  - PKI Certificate Integration
  - Verifiable Agent Identity
  - Trust Framework
  - Cross-Platform Interoperability
  - Secure Communication Enablement
  - Decentralized Discovery

[Submitted on 15 May 2025]

Agent Name Service (ANS): A Universal Directory for Secure AI Agent Discovery and Interoperability

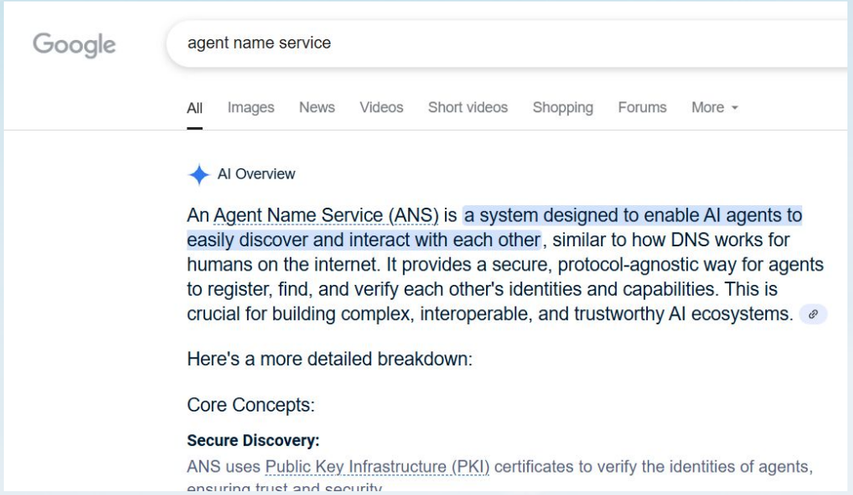
Ken Huang, Vineeth Sai Narajala, Idan Habler, Akram Sheriff

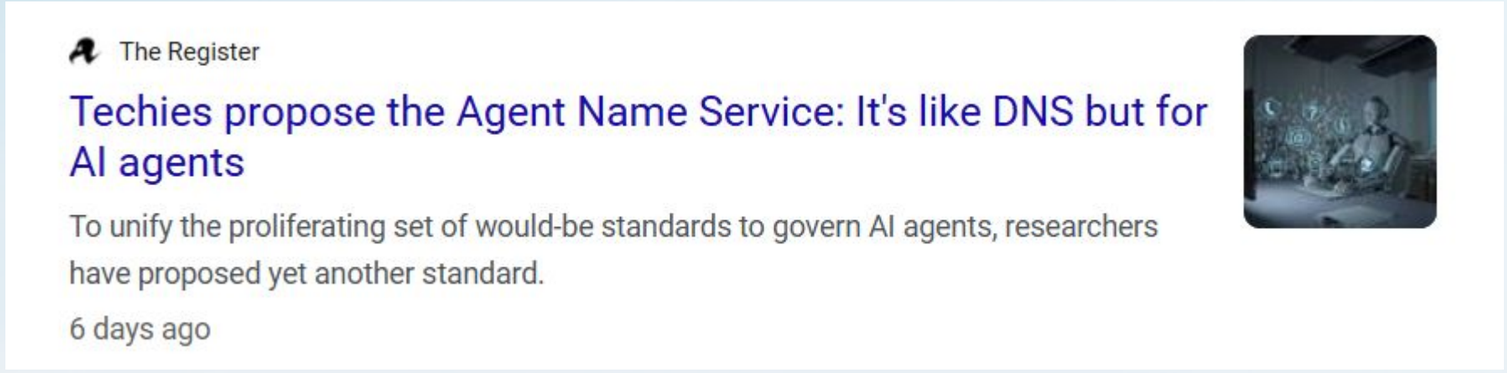
The proliferation of AI agents requires robust mechanisms for secure discovery. This paper introduces the Agent Name Service (ANS), a novel architecture based on DNS addressing the lack of a public agent discovery framework. ANS provides a protocol-agnostic registry infrastructure that leverages Public Key Infrastructure (PKI) certificates for verifiable agent identity and trust. The architecture features several key innovations: a formalized agent registration and renewal mechanism for lifecycle management; DNS-inspired naming conventions with capability-aware resolution; a modular Protocol Adapter Layer supporting diverse communication standards (A2A, MCP, ACP etc.); and precisely defined algorithms for secure resolution. We implement structured communication using JSON Schema and conduct a comprehensive threat analysis of our proposal. The result is a foundational directory service addressing the core challenges of secured discovery and interaction in multi-agent systems, paving the way for future interoperable, trustworthy, and scalable agent ecosystems.

Comments: 15 pages, 6 figures, 6 code listings, Supported and endorsed by OWASP GenAI ASI Project
Subjects: **Cryptography and Security (cs.CR)**; Artificial Intelligence (cs.AI); Multiagent Systems (cs.MA); Networking and Internet Architecture (cs.NI)
Cite as: arXiv:2505.10609 **[cs.CR]**
(or arXiv:2505.10609v1 **[cs.CR]** for this version)
https://doi.org/10.48550/arXiv.2505.10609

Submission history

From: Vineeth Sai Narajala [view email]
[v1] Thu, 15 May 2025 17:49:36 UTC (1,886 KB)

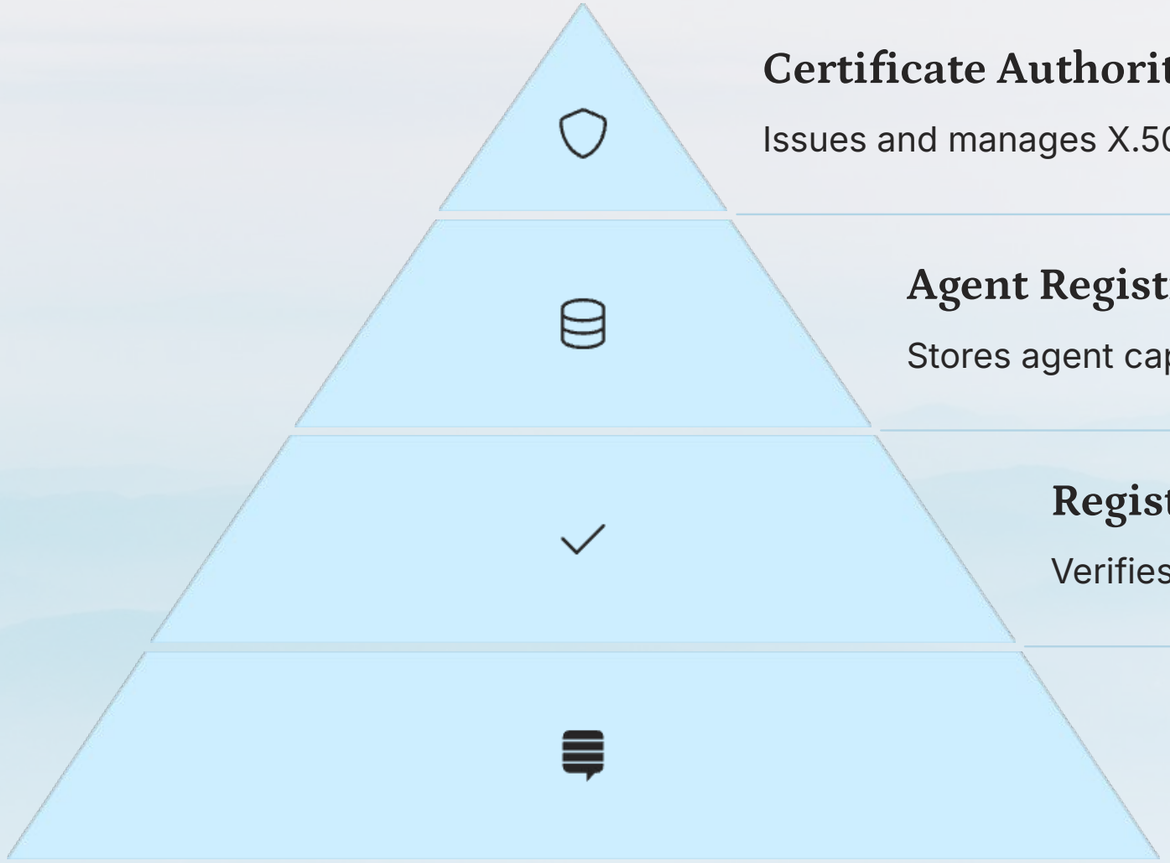




About Me: Ken Huang

- AI Book Author
- CSA Fellow
- Co-Chairs of Two CSA AI Safety Working Groups
- Core Member of OWASP top 10 for LLM Application
- Instructor of EC-Council on Generatie AI for Cyber Security
- CEO of DistrubutedApps.ai

Core Architecture Components



Certificate Authority

Issues and manages X.509 certificates

Agent Registry

Stores agent capabilities and credentials

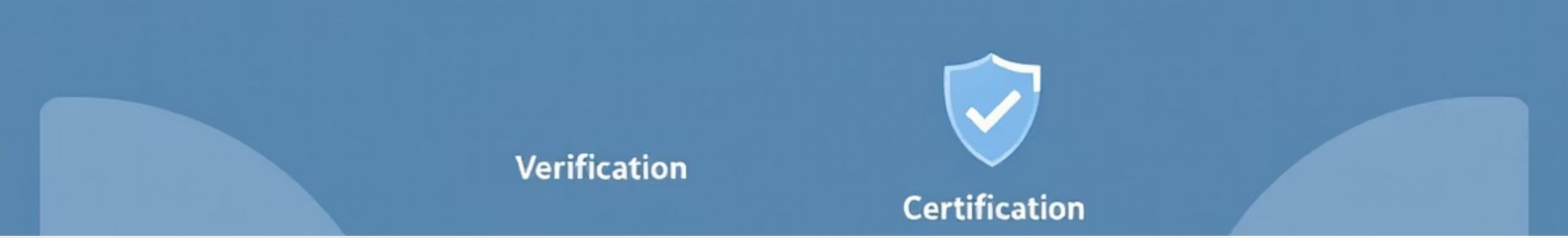
Registration Authority

Verifies agent requests and manages lifecycle

Protocol Adapter Layer

Translates between protocols

The ANS architecture features several key innovations: a formalized agent registration and renewal mechanism for lifecycle management; DNS-inspired naming conventions with capability-aware resolution; a modular Protocol Adapter Layer supporting diverse standards (A2A, MCP, ACP); and precisely defined algorithms for secure resolution.



Agent Registration Process

Submit Registration Request

Agent submits request with metadata, protocol details, and Certificate Signing Request (CSR)

Identity Validation

Registration Authority validates agent's identity and submitted information against registry policies

Certificate Issuance

RA requests certificate from Certificate Authority using validated CSR

Registry Storage

Certificate and agent information stored in Agent Registry with timestamp

ANS Naming Structure

The ANS naming structure provides a standardized way to identify and locate agents across different protocols and platforms. This structure encodes identity, capability, and contextual metadata in a format that facilitates discovery and verification.

Formal Structure

ANSName = Protocol "://" AgentID "." agentCapability "." Provider ".v" Version "." Extension

Example

a2a://textProcessor.DocumentTranslation.AcmeCorp.v2.1.hipaa

Components

- Protocol: Communication protocol (a2a, mcp, acp)
- AgentID: Unique agent identifier
- agentCapability: Primary agent capability
- Provider: Organization name
- Version: Semantic versioning format
- Extension: Optional metadata (e.g., compliance)

Resolution Process

Parse ANSName

Break down the ANSName into Protocol, AgentID, agentCapability, Provider, Version, and Extension components

Query Agent Registry

Search for agents matching the parsed components in the registry database

Version Negotiation

If multiple matches found, select the appropriate version based on compatibility requirements

Verify Endpoint Record

Validate the agent's endpoint record using cryptographic verification and certificate chain validation

Return Endpoint

Provide the verified endpoint information to the requesting agent for secure connection

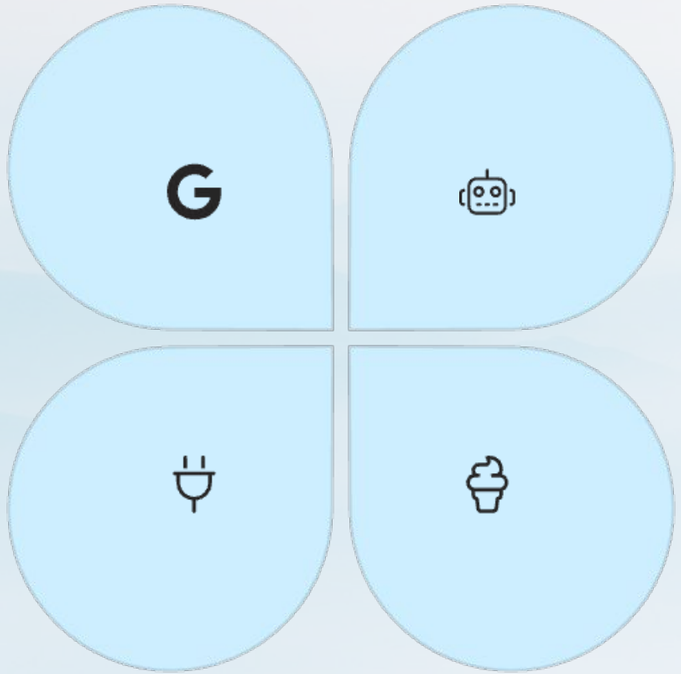
Protocol Adapter Layer

A2A Adapter

Parses Google's Agent2Agent Protocol information, enabling discovery based on A2A capabilities and facilitating endpoint location

Extension Points

Allows for adding support for new protocols through modular adapter interfaces



MCP Adapter

Handles Anthropic's Model Context Protocol, storing tool descriptions and enabling discovery of agents offering specific MCP tools/resources

ACP Adapter

Manages IBM's Agent Communication Protocol profiles, supporting discovery based on ACP roles and capabilities

Security Analysis

Threat	Risk	Mitigation Strategy
Agent Impersonation	Adversary attempts to impersonate a legitimate agent	Mandatory PKI implementation, certificate validation, digital signatures
Registry Poisoning	Injection of malicious data into Agent Registry	Strict RA validation, cryptographic signing of registry responses
Man-in-the-Middle Attacks	Modification of communications between components	Message authenticity/integrity via digital signatures, secure transport
Denial of Service	Attempts to incapacitate registry services	Distributed implementation design, rate limiting, DDoS protection

Demo

Future Directions

Prototype Implementation

Build and evaluate a working ANS prototype to validate the architecture and identify practical challenges: https://github.com/kenhuangus/ANS

Video: https://www.youtube.com/watch?v=_tO1JO_xLOk

Performance & Scalability

Benchmark resolution latency, registration throughput, and scalability under various load conditions

Advanced Cryptography

Investigate privacy-preserving techniques like zero-knowledge proofs for capability advertisement

Governance Model

Develop comprehensive policies for naming, CA/RA operations, disputes, and trust framework evolution

ANS offers a foundational infrastructure for a more secure, trustworthy, and interconnected agentic AI ecosystem. By enhancing interoperability, boosting trust and security, and accelerating innovation, ANS can become a critical enabler for the next generation of autonomous systems and secure AI marketplaces.