DNS-Centric Approaches to Agentic AI Identity Management

Nic Williams, nic@infoblox.com

Why DNS?

Portability: identity follows the domain, not the platform

- Vendor migration is one DNS edit (operator-owned / sovereignty)

Defense in depth: enforcement at multiple layers

- App-layer (WAFs, OAuth, API gateways) fires AFTER the request reaches the app
- DNS-layer (RPZ, protective DNS, DNSSEC, DANE) fires BEFORE the request leaves the resolver
  - Phishing, lookalike domains, tunnelling, C2 beaconing never reach the app
  - Compromised TLS cert or OAuth token still hits the app while a compromised DNS record fails DNSSEC validation

Existing governance plane: ~40 years of operational maturity (~500T daily queries, ~90%+ from cache)

- ICANN, registrars, dispute resolution, abuse reporting
- DNSSEC (cryptographic chain from root to zone)
- DANE / TLSA (anchors the TLS handshake in the same governed zone)

Cross-SDO Substrate Landscape

Venue	DNS-Centric	DNS-Dependent	DNS-Independent / Non-DNS
IETF	DNS-AID, DNSid, ARP, draft-cui-dns-native	ANS v2, AI Discovery Endpoint, AIDRE, Agent Directory, AGTP Discovery, AIP, did:web	AGNTCY SLIM, most OAuth/agent-token drafts
LF / AAIF	!!	!!	3 projects (MCP, goose, AGENTS.MD) & 7 candidate projects (Ferridis, Safe Zone, MCP Gateway Registry, OpenSandbox, AGT, Envoy AI, ACP)
LF / AGNTCY	!!	!!	All ~12 repos, dir uses content-addressing + DHT, not DNS
ITU-T (SG17 + SG20)	!!	!!	16 of 18 drafts: DIDs/VCs/ledger, X.509+OAuth+VC, agent registries, IoT platforms
AAIF-adjacent	—	AgentFinder (Google, AWS), DNS-dependent on publisher FQDN, HTTPS substrate	—

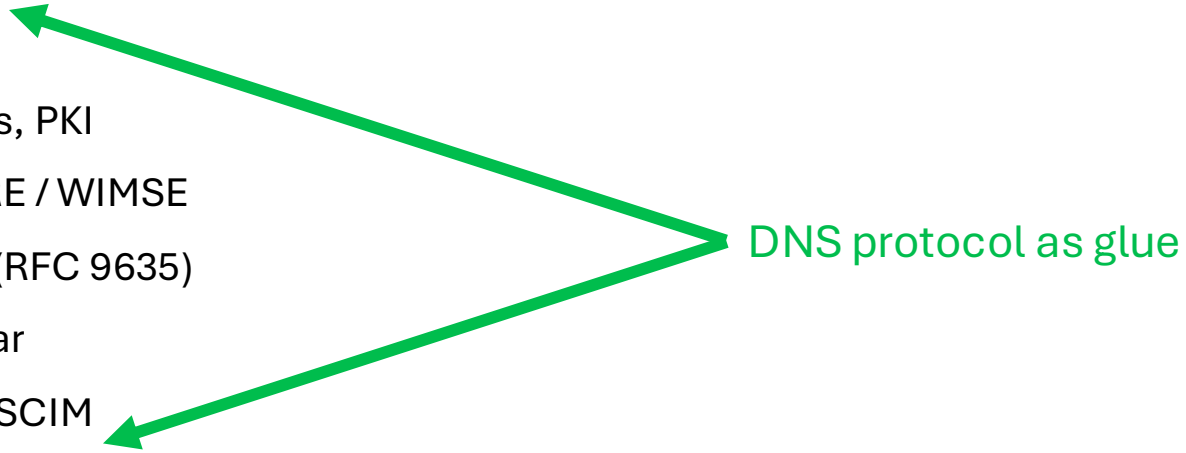
Problem Space Layers

- Layer 0 — Global namespace governance: ICANN, DNSSEC, DANE
- Layer 1 — Durable ownership anchor: ANS, DNSid
- Layer 2 — Cryptographic identity binding: ANS, DIDs, VCs, PKI
- Layer 3 — Runtime workload identity: SPIFFE / SPIRE / WIMSE
- Layer 4 — Authentication: OAuth 2.1, OIDC, GNAP (RFC 9635)
- Layer 5 — Authorization & policy: NGAC, OPA, Cedar
- Layer 6 — Operational governance: NHI platforms, SCIM
- Layer 7 — Discovery & interoperability: ANS, MCP, A2A, AGNTCY

Layer model: draft-ihsanullah-dnsid-00 §3.1 (Ihsanullah, Identity Digital)

Problem Space Layers

- Layer 0 — Global namespace governance: ICANN, DNSSEC, DANE
- Layer 1 — Durable ownership anchor: ANS, DNSid
- Layer 2 — Cryptographic identity binding: DIDs, VCs, PKI
- Layer 3 — Runtime workload identity: SPIFFE / SPIRE / WIMSE
- Layer 4 — Authentication: OAuth 2.1, OIDC, GNAP (RFC 9635)
- Layer 5 — Authorization & policy: NGAC, OPA, Cedar
- Layer 6 — Operational governance: NHI platforms, SCIM
- Layer 7 — Discovery & interoperability: MCP, A2A, AGNTCY



Layer model: draft-ihsanullah-dnsid-00 §3.1 (Ihsanullah, Identity Digital)

Recent DNS-Centric Proposals

Substrate IS DNS

- Resolvers retrieve agent state directly
- DNSSEC + DANE close the trust loop

DNS-AID (draft-mozleywilliams-dnsop-dnsaid-02)

- SVCB at <agent>.<zone>, walkable AliasMode, well-known + cap-sha256 + bap SvcParams

DNSid (draft-ihsanullah-dnsid-00)

- Ownership anchor, TXT at _dnsid.<agent-fqdn> (entity-signed)

ARP (draft-deforth-arp-00)

- Ed25519-signed claim binding via TXT at <selector>._arp.<domain>

(draft-cui-dns-native-agent-naming-resolution-01)

- A/AAAA + SVCB + TXT, private SvcParams for version + protocols

Recent DNS-Dependent Proposals

DNS gets you to the host (”let the application handle it”)

- Substrate (state, identity, history) lives in HTTPS, ledger, or registry

ANS v2 (draft-narajala-courtney-ansv2-01)

- Tri-channel: _ans + _ans-badge TXT hints, transparency-log proofs, HTTPS verify APIs

AI Discovery Endpoint (draft-aiendpoint-ai-discovery-00)

- Pure HTTPS well-known at /.well-known/ai

AIDRE (draft-batum-aidre-00)

- HTTPS well-known at /.well-known/ai-discovery (MUST NOT require DNS-SRV)

Agent Directory (draft-jimenez-agent-directory-01)

- Centralized HTTP/JSON directory adapted from CoRE Resource Directory

AGTP (draft-hood-agtp-discovery-00) + AIP, did:web variants

- Federated ANS / registry / DID-based, varying trust + governance models

Chose Non-DNS Substrates

AAIF (Linux Foundation): zero DNS-centric projects, all formal + 7 candidates are app-layer

- Formal: MCP, goose, AGENTS.MD — all DNS-independent
- Candidates: Ferridis, Safe Zone, MCP Gateway Registry, OpenSandbox, Agent Governance Toolkit, Envoy AI Gateway, ACP

AGNTCY (LF, Cisco-led, 65+ supporting orgs): deliberately picked away from DNS

- Agent Directory (dir): content-addressing + DHT (no DNS, no central registry)
- Identity: cryptographic-key-based, not DNS-anchored
- SLIM: gRPC + HTTP/2 + MLS, OASF: schema framework

AAIF-adjacent: AgentFinder (Google, AWS): DNS-dependent on publisher FQDN, HTTPS substrate

Pipeline (Same Gap)

- 18 SG17 + SG20 agentic-identity contributions surveyed (keywords: AI, agent, agentic)

- Elixir Mgmt (Vasylenko, Ukraine) — 5 contributions, Q10 + Q16/17
  - X.gaiv, X.aaid, X.rcae, X.atcp, X.aam: X.509 + W3C VCs + OAuth/OIDF + FIDO
- Korea (Youm / Park / Hyeon) — 2 contributions, Q10/17
  - X.dpidm-aAI: "global uniqueness (DNS for example) is not strictly required"
  - X.id-AA-dis: DIDs + VCs over verifiable data registry / DLT, not did:web, GNAP authz
- India DoT (Manaswi et al.) — 3 contributions, Q16/17
  - X.sg-dp, X.sg.aai, X.dac-aa: agent registry + provenance (app-layer, not DNS)
- SG20 liaisons (Y.IoT-dAIA, Y.AIA-SO) — IoT-platform-centric, DNS-independent

Pipestrat (Study Group)

- 18 SG17 + SG20 agentic-identity contributions surveyed (keywords: AI, agent, agentic)
- Elixir Mgmt (Vasylenko / Ukraine) — 5 contributions, Q16→Q16/17
  - X.gaiv, X.aaid, X.rcae, X.atcp, X.aam: X.509 + W3C VCs + OAuth/OIDF + FIDO
- Korea (Youm / Park / Hyeon) — 2 contributions, Q16/17
  - X.dpidm-aAI: "global uniqueness (DNS for example) is not strictly required"
  - X.id-AA-dis: DIDs + VCs over verifiable data registry / DLT, not did:web, GNAP authz
- India DoT (Manaswi et al.) — 3 contributions, Q16/17
  - X.sg-dp, X.sg.aai, X.dac-aa: agent registry + provenance (app-layer, not DNS)
- SG20 liaisons (Y.IoT-dAIA, Y.AIA-SO) — IoT-platform-centric, DNS-independent

DNS-substrate discussion appears ONLY in two meta docs

TD-PLEN-0284 SG17 Chair status deck

TD-PLEN-0261 TSB Workshop Report

Both cite Ken Huang ANS, China Mobile "DNS for IoA," DNS-AID family externally

infoblox. ITU

Where This Workshop Can Help

- SG17 named the gap (TD-PLEN-0234, TD-PLEN-0261)
  - No current draft Recommendation embodies DNS-substrate work
  - No ITU-T draft cites DNS-AID, DNSid, ARP, or ANS-v2 by IETF draft name

- Potential action items for Q10/17
  - New work item for DNS-substrate identification + discovery, complement-framed against existing Q10/17 work
  - Liaison to IETF on developing Working Groups for AI
  - Reference incorporation into X.dpidm-aAI baseline (recognize DNS as one valid substrate)
  - Slide 9 ITU contribution drafts can sit on top / anchor on

- Action items for workshop attendees
  - Recognize and discuss the layer model (Layer 0/1 are DNS-native; Layer 2–6 stack above)
  - Recognize the substrate fork: LF chose away from DNS, IETF may leverage it, ITU-T TBD

Why DNS?

Practicality

- BGP glues together the networks making up the Internet, DNS facilitates everything communicating over it… these are the two "glue" protocols of the internet.
- Largest scale of deployed federated /decentralized protocols (~500T daily queries,~10^104 total namespace permutations).
- Leverage existing technology expertise /employees: developers, vulnerability community, enterprises use and integrate to existing technologies to current network stack.
- Reduce internet fragmentation utilizing all the above to give AI workloads a known entry point to organizations using existing digital trust boundaries (domain + certificates a la DNSSEC,DANE, mTLS, etc.)… right now 😎 .

Governance

- Root zone operation / control federated across borders.
- Diversity of hosting options across TLDs, registrars, registries, and even the hosting infrastructure.
- *Accepted universal domain takedown process (UDRP).*
- Increase individual operator sovereignty while decreasing third-party reliance: organizations advertise their own services without the risk of opaque registry rules or business practice (i.e. paid placement of less-reputable agents), delegate authority to business partnerships without need for registry approval.
- Organizations have sovereignty, the alternative might be commercial agent registries.

nic@infoblox.com