C=US National Identity

An X.500 registry for people and AI agents, distinct from the Federal Bridge PKI

PSU Student | AI-285 | cequs.com | Peter Bachman

Maple agent mock

Separate infrastructure. A national registry with rights principles.

The Federal Bridge PKI certifies trust between certificate authorities. This concept defines a national registry for person and AI-agent identities.

AI being used in use case: Maple Sugar Agent Grading

Codex/Astra designed this use case and configured the OpenLDAP schema as an X.500 stand-in. Codex then mocked the maple-syrup grading web page. n8n is designed to perform the LDAP query for the page, validate the directory-registered agent, and gather spectrometry-analyzer data installed at a maple-sugar farm. This is one use case; the wider project is agentic-registration infrastructure.

State agricultural AI use case: maple syrup

For Vermont and Quebec supply chains, McGill research paired portable Raman spectroscopy with deep learning to estimate maple syrup total phenolic content and antioxidant capacity on site [9]. A registered agent can bind device, grove, lot, grade, provenance, and authorized business rules to long-running quality loops. The study evaluates syrup samples, not tree-level measurements.

National scope, state focused

The proposal registers agents in participating states. For Maple Syrup Grading, Vermont is under c=US and Quebec is under c=CA. Registry data is based on Utah Self-Endorsed Digital Identity concepts.

HAPPY PATH

AI agents receive high-value identity and authorization scope only through explicit, time-bounded grants.

SAD PATH

A sandbox escape in an organizational AI environment, admin credential theft, or production-server takeover triggers containment, revocation, and incident response.

Namespace basis

1.3.6.1.1 is the Internet Directory OID arc [2]. It supports directory schema assignments. c=US is the country branch in the illustrative X.500 tree.

Illustrative identity directory subtree

c=US / o=Example Endorser / ou=AI-Agents

02 Rights-preserving architecture

1 State or other endorser

Verifies eligible attributes and endorses a holder-controlled identity.

LDAP access: authorized updates, no usage trail

2 X.500 Registry: c=US

Cooperating DSAs publish approved registry entries for people and AI agents.

LDAP access: protected, policy-limited responses

3 Holder-controlled credential

Presents selected attributes without routine verifier contact to the endorser.

Approved attributes, purpose-limited use

4 Relying service

Checks the presented credential and applies a documented access policy.

LDAP provides access to the X.500 Registry [3]. Registry access is policy-limited, and holders present selected attributes without creating a log of every use.

03 Consulting, IP & governance

Integration architecture

Link the X.500 / LDAP Directory with Okta, OAuth and OpenID Connect, Microsoft Entra ID, and other identity and authorization frameworks. Design secure human and agentic identity workflows.

Compliance & risk mapping

Map controls, evidence, data flows, and role boundaries across GDPR, CCPA, HIPAA patient identity and covered-entity obligations, ISO/IEC 27001, SOC 2, NIST SP 800-64, PCI DSS, CIS Controls, and TBD agentic AI requirements.

Open standards & creative IP

Published open systems standards support interoperability. Creative contributions, including schema profiles, policy maps, workflow designs, and tools, remain subject to their creators' intellectual property rights.

Negotiated IP carveout

Each participant is invited to negotiate a carveout that preserves its pre-existing and independently created IP. Licenses for contributions, integration deliverables, and the c=US structure must be explicit.

c=US provenance position

The asserted basis is the original 1993 NSF Directory Grant, the PSINet White Pages Project, and a Department of Commerce negotiation at project close. c=US maintains IP in the negotiated overall structure. Confirm grant and agreement terms before reliance.

STUDENT AI AND THIRD-PARTY DISCLOSURE

AI-assisted AI-285 course work prepared by a PSU student for conceptual and educational discussion. It is not Penn State policy, legal advice, a production offering, or an independently validated design. Third-party names identify possible integration contexts only. Their marks belong to their respective owners; no named organization has participated in, sponsored, endorsed, approved, or adopted this work.

REFERENCES

[1] FPKI. Federal Bridge CA policy and cross-certification framework. idmanagement.gov/fpki
[2] IETF. Internet Directory OID arc 1.3.6.1.1. RFC 1155. rfc-editor.org/rfc/rfc1155
[3] IETF. RFC 4511. LDAP access to X.500 Directory services. rfc-editor.org/rfc/rfc4511
[4] IETF. RFC 4513. LDAP authentication and security. rfc-editor.org/rfc/rfc4513
[5] NIST. SP 800-63-4. Digital Identity Guidelines. doi.org/10.6028/NIST.SP.800-63-4
[6] Utah Code, Title 63A, Ch. 20. State-Endorsed Digital Identity. le.utah.gov
[9] Xiao et al. Food Chemistry 463 (2025) 141289. doi.org/10.1016/j.foodchem.2024.141289