C=US National Identity

An X.500 Directory concept, distinct from the Federal Bridge PKI

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

Separate infrastructure. Shared trust and rights principles.

The Federal Bridge PKI certifies trust between certificate authorities. This concept addresses rights-preserving identity discovery and verification.

01 Two different systems

Existing Federal Bridge PKI [1]

The Federal Bridge Certification Authority is an established X.509 interoperability bridge. It cross-certifies Principal Certification Authorities to create certificate trust paths under c=US,o=US Government.

Proposed identity directory

This concept is separate. It organizes approved identity attributes in an X.500 Directory. LDAP is an access protocol to that Directory. It does not change the Federal Bridge PKI or turn certificate cross-certification into a national person registry.

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. Neither identifier proves citizenship, assurance, or government endorsement.

Illustrative identity directory subtree

c=US
└ o=Example Endorser
  └ ou=People

Example distinguished name (LDAP notation)

uid=p1042,ou=People,
o=Example Endorser,c=US

Illustrative names only. Naming does not define access rights.

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 Directory: c=US
Cooperating DSAs publish the minimum approved directory attributes.

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 Directory [4]. This design does not use the Federal Bridge PKI as a person directory. A holder can present selected attributes without making the Directory a log of every use.

Design basis: NIST roles [5]. Utah SEDI rights principles [6].

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.

Each engagement confirms applicability, shared responsibility, evidence requirements, and IP terms with the client, counsel, assessors, and regulators.

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
[7] OHCHR. Human rights and digital technologies. ohchr.org
[8] PSINet White Pages provenance statement. alvestrand.no/objectid/1.3.6.1.1.html