ALLDISPATCH
@IETF121

draft-carter-high-assurance-dids-with-dns

https://datatracker.ietf.org/doc/draft-carter-high-assurance-dids-with-dns/

Jesse Carter (CIRA), Jacques Latour (CIRA),
Tim Bouma (Digital Governance Council), Mathieu Glaude (Northern Block)

IETF

What is a High-Assurance DID with DNS?

Building on the rock-solid backbone of DNS and DNSSEC, we're bringing decentralized identifiers (DIDs) into a globally recognized, unique, and accessible namespace.

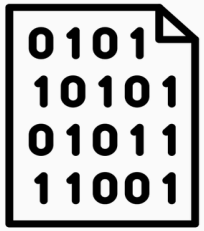
Human-Readable Identifier

did:web:issuer.example.ca

Machine-Verifiable Assertions

- Digital Certificates and Signatures
- DID Document DataIntegrityProof
- DNS/DNSSEC Validation
  - DANE TLS Check
  - DID URI Record Match
  - TLSA Self-Issued Certificate Record Match
- Member of Trust Registry

+



Human Trust

Technical Trust

Motivation

Highlight	Value Proposition
Leverages DNS/DNSSEC	Builds on proven infrastructure (DNS and DNSSEC) as a trusted backbone.
Bridges Old and New	Connects well-known internet protocols with the evolving digital trust (decentralized identity/credential) landscape.
Enhances Trust and Assurance	Anchors public keys in DNS with DNSSEC for high-assurance interactions across all document types.
Increases Discoverability and Interoperability	Offers a globally recognized namespace to support seamless use across platforms.
Flexible, Tech-Agnostic Solution	Maps public keys for issuers of any digital credential type (e.g., PKI x509, mDL, W3C, AnonCreds), not tied to specific technology.
Strengthens Digital Identities	Creates a universal pattern for reliable, decentralized identity verification using and leveraging the unique identifiers of the DNS.

Background

Institutions are realizing that their trusted domain name (i.e., website) can be now leveraged to become a 'trusted identifier' that can cryptographically sign and verify documents and credentials.

E.g., "agency.gov" can now sign with "did:web:agency.gov".

Adoption and Implementations;

DHS Implementation:

- *https://dhs-svip.github.io/requirements-for-decentralized-identity/TrustArchitecture/*

DIF Trust DID Web Decentralized Identity Foundation:

- *https://identity.foundation/trustdidweb/*

Trust Over IP Foundation High Assurance VID Task Force

- *https://lf-toip.atlasian.net/wiki/spaces/HOME/pages/32473104/High+Assurance+VID+Task+Force+HAVIDs*

IETF

Background

Who Would Want to Advance DNS-based High-Assurance DIDs?

Interested Parties	Interest
Digital Identity Standards Groups	Organizations like DIF, W3C, and OpenID, looking for trusted, tech-agnostic identity solutions.
IETF Security & DNS Working Groups	Aligns with DNSOP, SEC, and TLS groups focused on secure, interoperable DNS innovations.
Governments & Public Authorities	National ID initiatives (e.g., eIDAS, mDL) needing a globally recognized, high-assurance identifier.
PKI & Certificate Authorities	Bridges X.509 and other credentials, reinforcing PKI's role in multi-credential ecosystems.

IETF

Hoped-for dispatching outcome

***Direct the work to an existing WG**: Leveraging current expertise in DNS/DNSSEC and digital credentials.*

***Propose a new focused WG**: Dedicated group to explore DNS-based high-assurance DIDs and cross-credential interoperability.*

***Recommendation to hold a full BOF**: Engage broader IETF stakeholders to assess interest and refine goals for high-assurance digital credentials.*

***Preferred Outcome:** Existing WG*