The Challenge of Using ‘the’ DNS in ‘a’ Digital Credential World

ICANN DNS Symposium
(Da Nang, Vietnam)
Sept 5, 2023

Presented By
Jacques Latour – CIRA
A TRUST LAYER IS EMERGING

The Trust Over IP Foundation

• We’re an independent project hosted at the Linux Foundation, working with pan-industry support from leading organizations around the world.
• Our mission is to provide a robust, common standard and complete architecture for Internet-scale digital trust.

The mission of the Trust over IP (ToIP) Foundation is to define an overall architecture for Internet-scale digital trust that combines cryptographic assurance at the machine layers (technology) with human accountability at the business, legal, and social layers (governance). https://trustoverip.org/our-work/technical-architecture/Together these two halves form a complete four-layer architecture for decentralized digital trust infrastructure known as the ToIP stack

https://trustoverip.org/our-work/technical-architecture/
ToiP Technology Stack

Application Ecosystems

Layer 4

Trust Task Protocols
Example: Credential Exchange

Layer 3

Peer-to-Peer Communication

Layer 2

Public Utilities

Layer 1

ToiP Governance Stack

Ecosystem Governance Frameworks

Layer 4

Trust Task Governance Frameworks

Layer 3

Agent/Wallet Governance Frameworks

Layer 2

Utility Governance Frameworks

Layer 1

cira

Governing Authority

Ecosystem Framework

Governs/Certifies

Governing Authority

Credential Framework

Governs/Certifies

Governing Authority

Agent/Wallet Framework

Governs/Certifies

Governing Authority

Utility Framework

Governs/Certifies

Governing Authority

Utility Provider Roles

Governs/Certifies

Governing Authority

Agent/Wallet Provider Roles

Governs/Certifies
A TRUST LAYER IS EMERGING

The ToIP Trust Spanning Protocol

Extracted from an August 2001 presentation by Steve Deering of Cisco, illustrates how the TCP/IP stack implements the Hourglass Model.

The hourglass model as implemented by the TCP/IP stack

https://www.trustoverip.org/blog/2023/01/05/the-toip-trust-spanning-protocol/
A TRUST LAYER IS EMERGING

How the hourglass model applies to the ToIP stack

https://www.trustoverip.org/blog/2023/01/05/the-toip-trust-spanning-protocol/
WHY DO I CARE SO MUCH ABOUT THIS? (It’s the technology direction)

The really cool part is the DIDComm “Secure Connection”

We need to pay attention to development around DIDComm V2 and the impacts on DNS usage

- https://identity.foundation/didcomm-messaging/spec/
A TRUST LAYER IS EMERGING

Digital Credentials \(\approx\) Decentralized and Verifiable Identifiers

https://www.trustoverip.org/blog/2023/01/05/the-toip-trust-spanning-protocol/
Example of a digital credentials: A Driver’s license

"Issuer": "did:key:z6Mkjxv...Fgy2E5"
"issuanceDate": "2023-01-15T10:00:00"
"expirationDate": "2026-08-27T12:00:00"
"credentialSubject":
  "id": "did:example:12347abcd"
  "license":
    "type": "Iso18013DriversLicense"
    "document_number": "D6101-40707-60905"
    "family_name": "DOE"
    "given_name": "JOHN"
    "portrait": "/9j/....5HtRRSClooooP/2Q=="
    "birth_date": "1998-08-28"
    "issuing_country": "CA"
    "issuing_authority": "ON",
"proof":
  "type": "Ed25519Signature2020",
  "verificationMethod": "did:key:z6Mkjxv...Fgy2E5#key1" (public key)
  "proofValue": "z4zKSH1WmuSQ8tcpS...FaiLvBUjJ89GP7V" (signature)
DIGITAL CREDENTIAL DECENTRALIZATION

Example of a decentralized Identifier (DID): Driver’s licenses issuer

```json
"@context": [
  "https://www.w3.org/ns/did/v1",
  "https://w3id.org/security/suites/ed25519-2020/v1",
],
"id": "did:key:z6Mkjxv...Fgy2E5"
"services": [{
  "type": "LinkedDomains",
  "serviceEndpoint": "https://serviceontario.ca"
}]
"verificationMethod": [
  {
    "type": "Ed25519VerificationKey2020",
    "id": "did:key:z6Mkjxv...Fgy2E5#key1"
    "controller": "did:key:z6Mkjxv...Fgy2E5"
    "publicKeyBase58": "HdXo5kegxPze3tAw6QY...sB6eS"
  }
]
"authentication": ["did:key:z6Mkjxv...Fgy2E5#key1"]
"assertionMethod": ["did:key:z6Mkjxv...Fgy2E5#key1"]
```
Another example of a digital credential

```
"issuer": "did:sov:y7kWjxv...Ggy3E4"
"issuanceDate": "2023-01-11T10:00:00"
"expirationDate": "2033-08-27T12:00:00"
"credentialSubject":
  "id": "did:example:12347abcd"
  "degree":
    "issuing_authority": "Zoom University"
    "issuing_country": "USA"
    "degree_type": "Bachelors of Computer Science"
    "gpa": "4.0"
    "family_name": "DOE"
    "given_name": "JOHN"
    "birth_date": "1998-08-28"
"proof":
  "type": "Ed25519Signature2020",
  "verificationMethod": "did:sov:y7kWjxv...Ggy3E4#key1" (public key)
  "proofValue": "z4zKSH1WmuSQ8tcpS...FaiLvBUjJ89GP7V" (signature)
```
Another example of a DID: A university diploma issuer

```
"@context": [
  "https://www.w3.org/ns/did/v1",
  "https://w3id.org/security/suites/ed25519-2020/v1",
],
"id": "did:sov:y7kWjxv...Ggy3E4"
"services": [{
  "type": "LinkedDomains",
  "serviceEndpoint": "https://zoom-university.io"
}]
"verificationMethod": [
  {
    "type": "Ed25519VerificationKey2020",
    "id": "did:sov:y7kWjxv...Ggy3E4#key1"
    "controller": "did:sov:y7kWjxv...Ggy3E4"
    "publicKeyBase58": "HdXo5kegxgPze3tAw6QY...sB6eS"
  }
]
"authentication": ["did:sov:y7kWjxv...Ggy3E4#key1"]
"assertionMethod": ["did:sov:y7kWjxv...Ggy3E4#key1"]
```
GLOBAL INTEROPERABILITY AND UNIQUE IDENTIFIERS

Experimentation so far has demonstrated DNS can be a great mechanism to facilitate the DID discovery process and reinforce trust.

- There needs to be global interoperability between all the different governance ecosystems:
  - ToIP identifiers need to be unique
- For an Issuer, map a domain name in a DID (W3C DID core spec)
  - Map a domain name via “alsoKnownAs” or “serviceEndpoint” fields
- Leverage the DNS for Issuer and Trust Registry discovery
  - Map the DID to a domain name
  - Map the DID public key to a TLSA (like) record
  - Map the Trust Registry affiliation/registration to the DNS
  - Standardise globally on the use of URI, PRT, TLSA and Labels

+DNSSEC everywhere!!!
CONCLUSION

Digital Credentials in Canada and abroad is a real thing
ToIP is evolving real time – See if you can contribute
Let’s make the DNS relevant in Digital Trust

• Looking at standardizing development efforts at IETF 118 Prague
  • No standards yet on the use of DNS in this world
  • Planning some meetings at Prague IETF - not ready for BoF
Thank You

https://www.cira.ca
EXPERIMENTAL REFERENCES:

Some relevant presentations and github repos

- 2.2 CIRA ICANN76 DNSSEC Workshop DID To DNS V2
- 5. CIRA ICANN76 Tech Day .CA Verified Domain PoC
- https://github.com/CIRALabs/DNS-Based-VCs-and-Trust-Registries-ID
- https://github.com/CIRALabs/TrustyDID