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

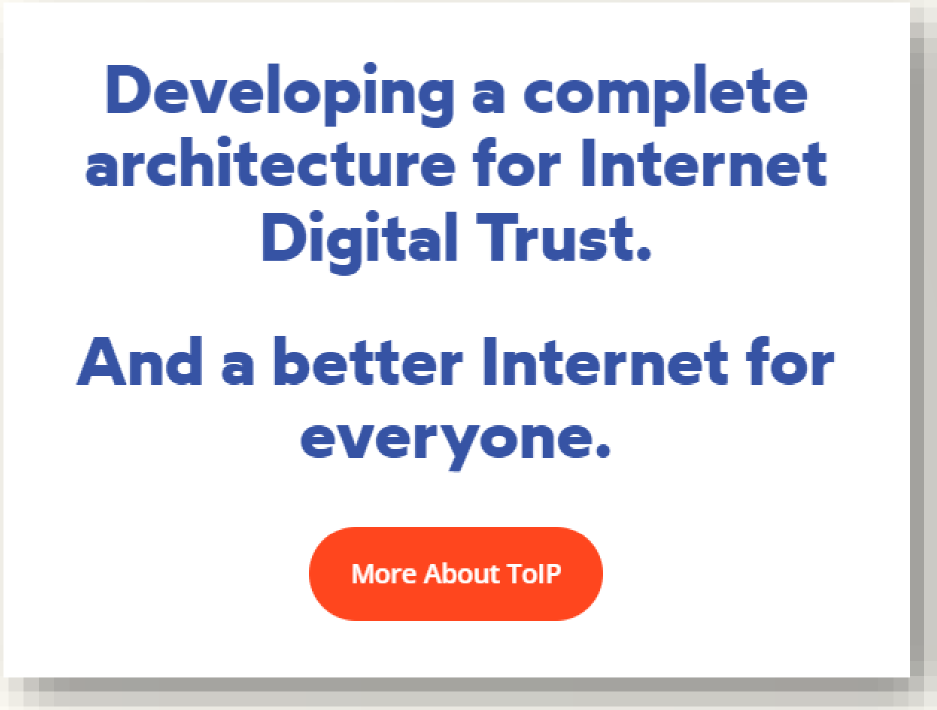
cira

CLASSIFICATION:PUBLIC

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.

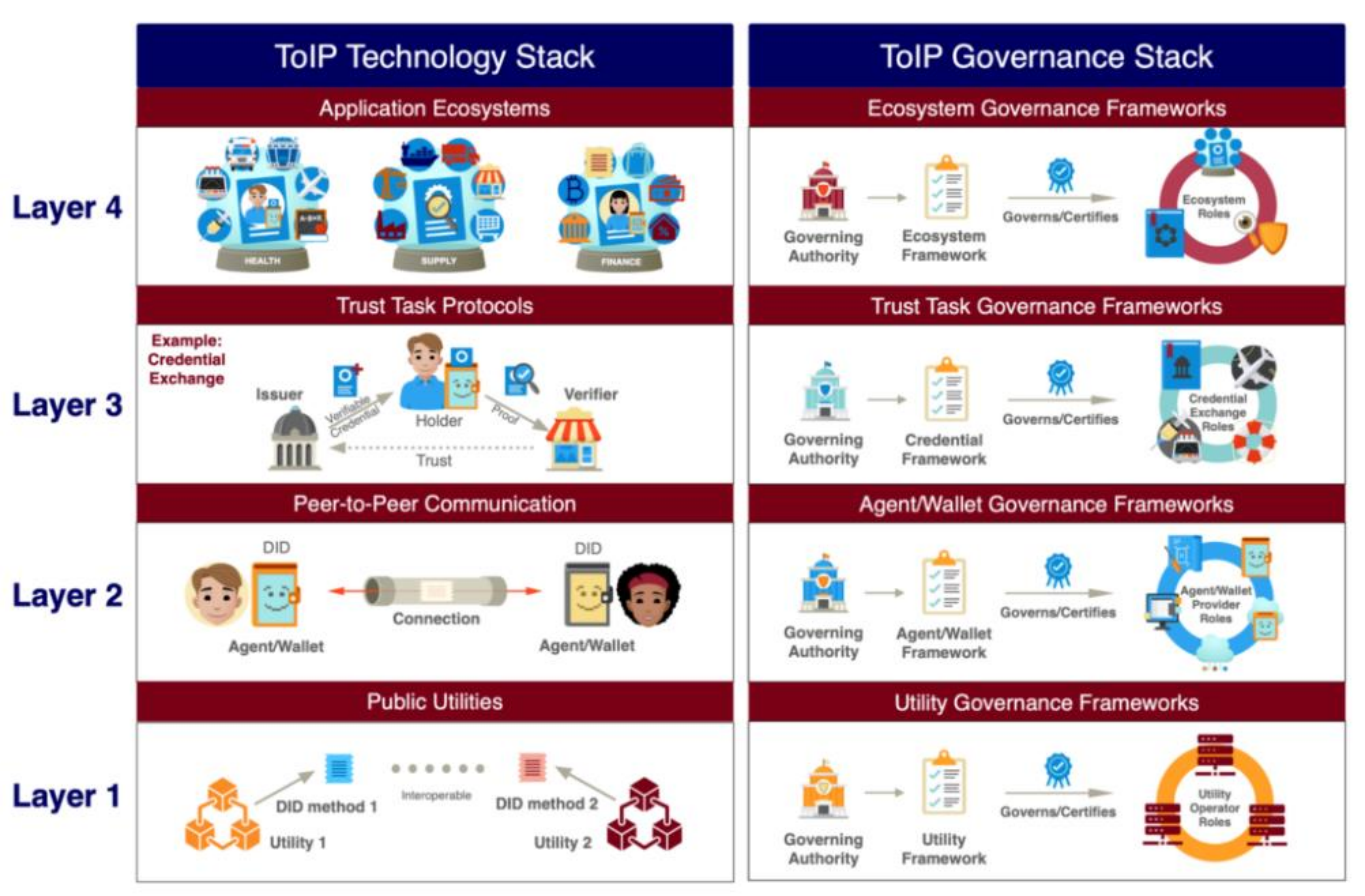


Developing a complete architecture for Internet Digital Trust.

And a better Internet for everyone.

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**

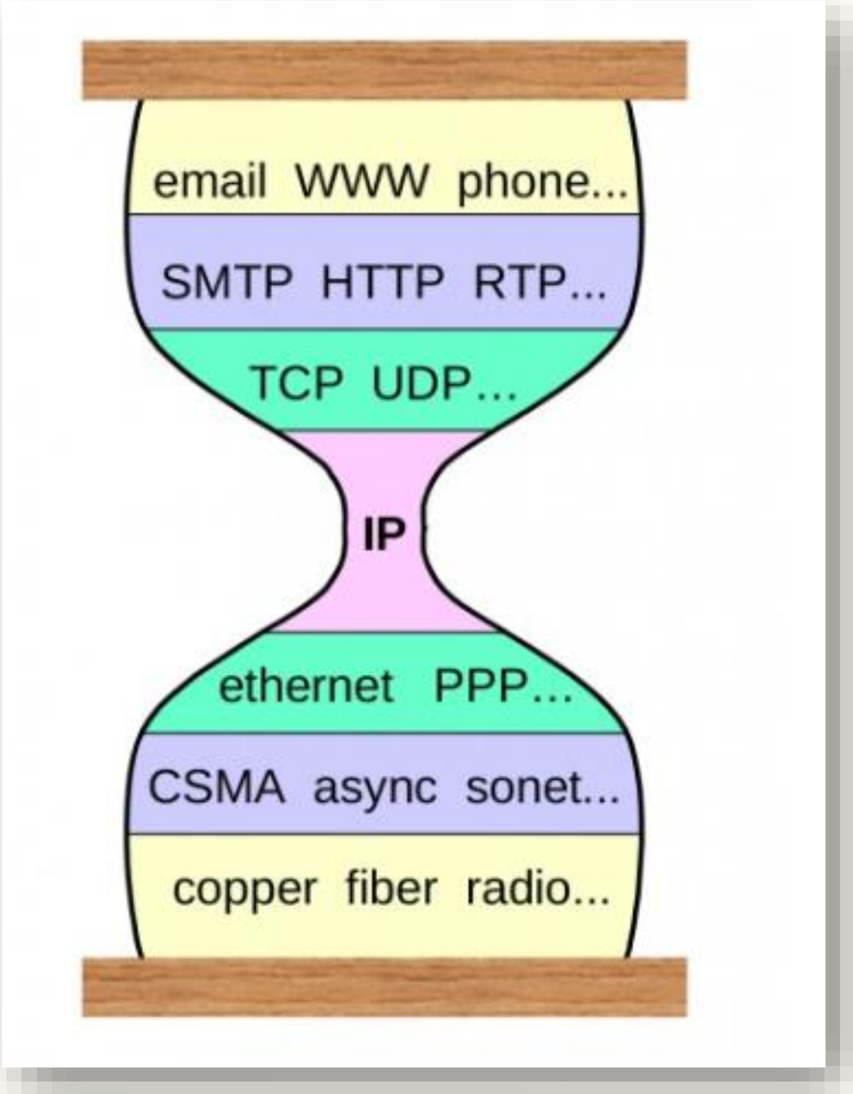
https://trustoverip.org/our-work/technical-architecture/



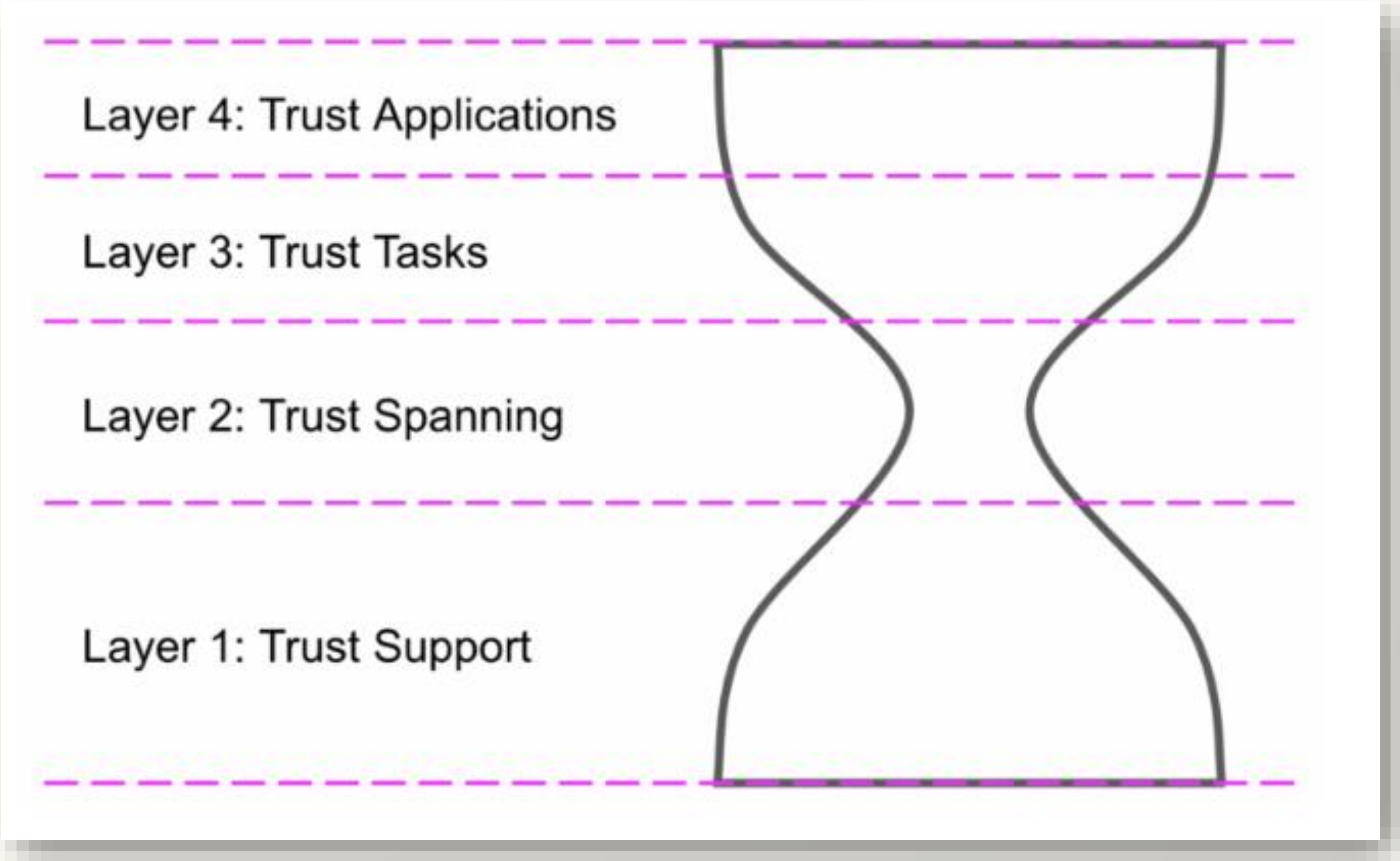
	ToIP Technology Stack	ToIP Governance Stack
Layer 4	Application Ecosystems	Ecosystem Governance Frameworks
Layer 3	Trust Task Protocols	Trust Task Governance Frameworks
Layer 2	Peer-to-Peer Communication	Agent/Wallet Governance Frameworks
Layer 1	Public Utilities	Utility Governance Frameworks

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.

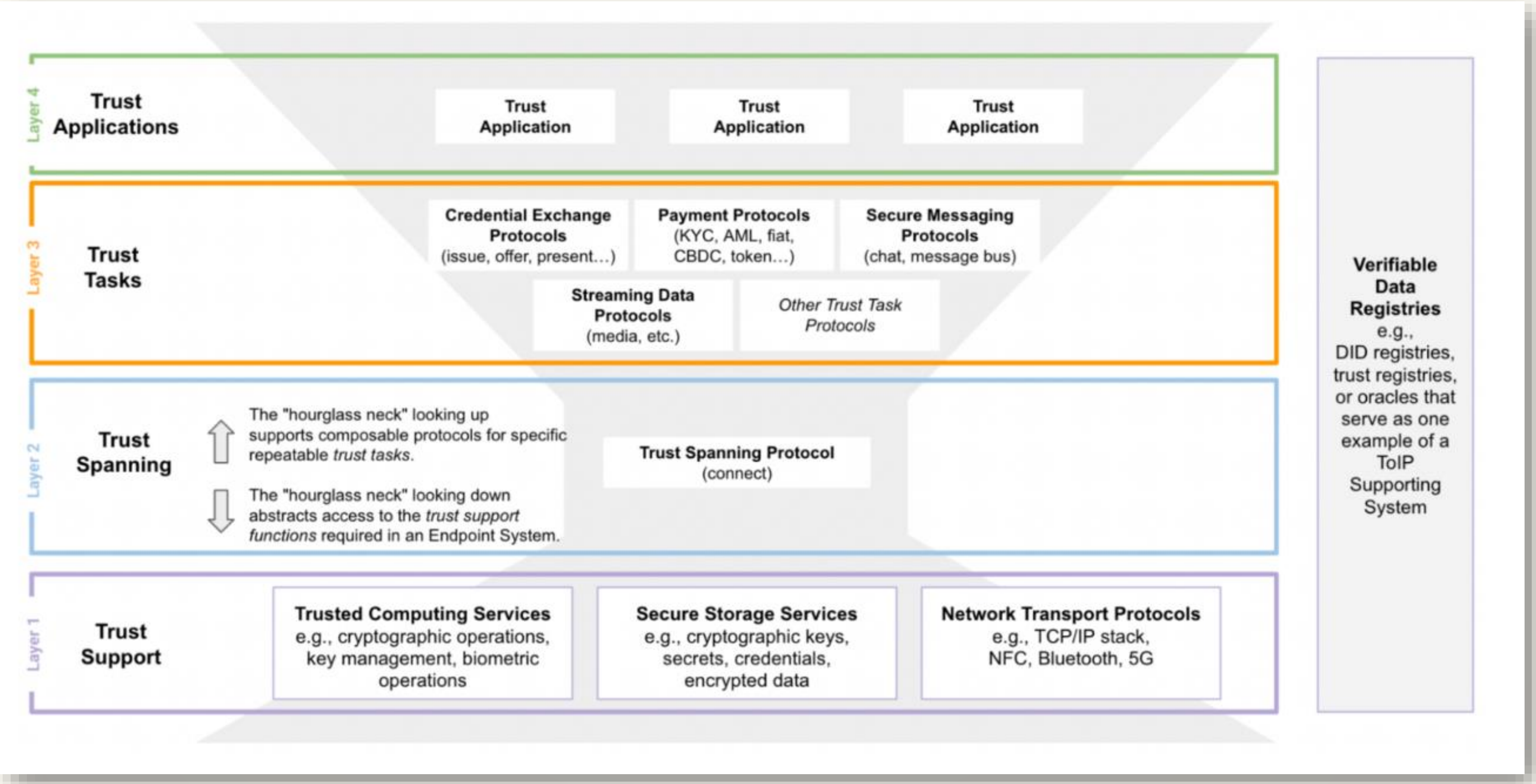


The hourglass model as implemented by the TCP/IP stack

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



Layer 4 — **Trust Applications**

Trust Application | **Trust Application** | **Trust Application**

Layer 3 — **Trust Tasks**

Credential Exchange Protocols (issue, offer, present…)

Payment Protocols (KYC, AML, fiat, CBDC, token…)

Secure Messaging Protocols (chat, message bus)

Streaming Data Protocols (media, etc.)

Other Trust Task Protocols

Layer 2 — **Trust Spanning**

⇧ The "hourglass neck" looking up supports composable protocols for specific repeatable *trust tasks*.

⇩ The "hourglass neck" looking down abstracts access to the *trust support functions* required in an Endpoint System.

Trust Spanning Protocol (connect)

Layer 1 — **Trust Support**

Trusted Computing Services e.g., cryptographic operations, key management, biometric operations

Secure Storage Services e.g., cryptographic keys, secrets, credentials, encrypted data

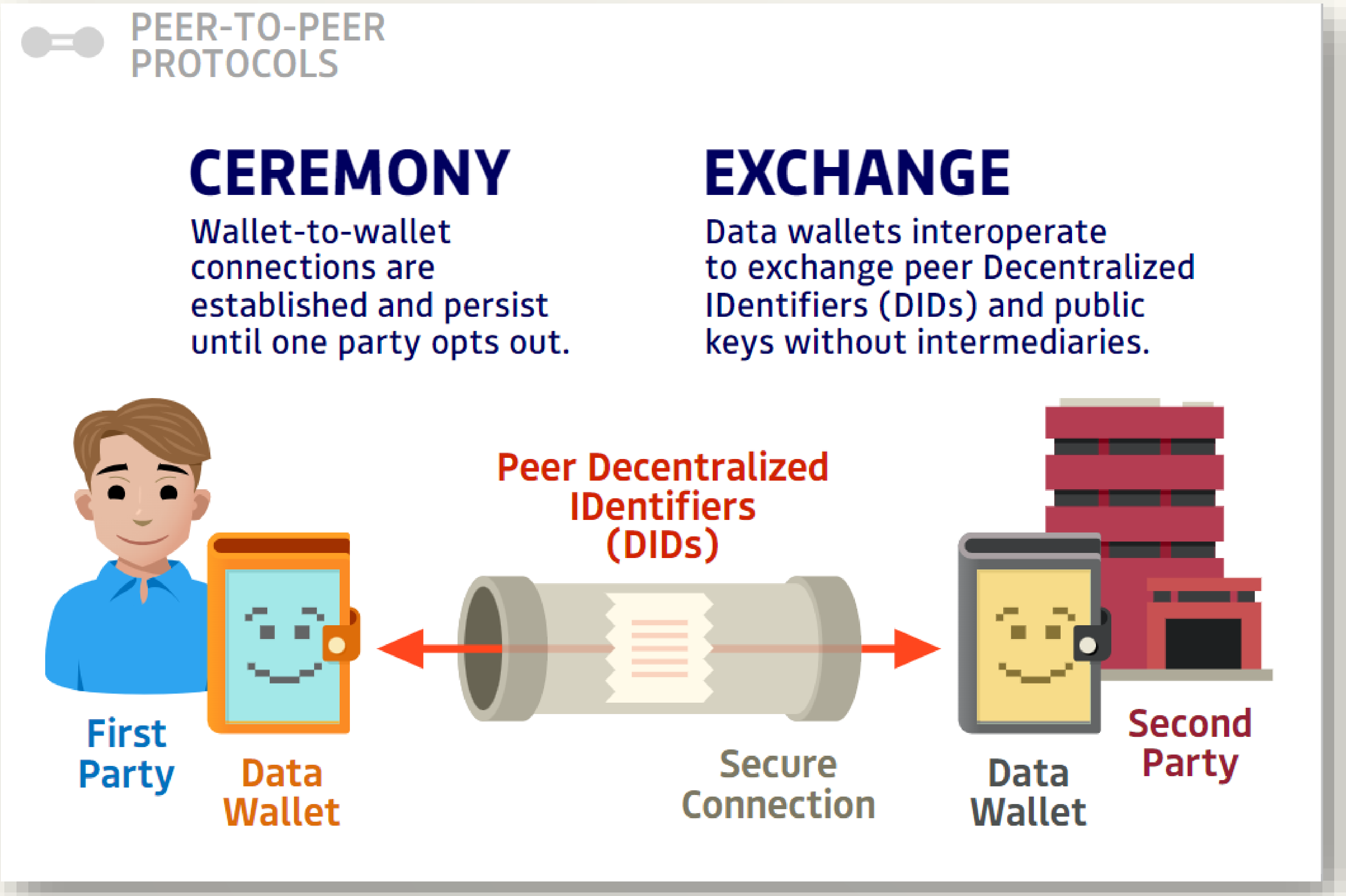
Network Transport Protocols e.g., TCP/IP stack, NFC, Bluetooth, 5G

Verifiable Data Registries e.g., DID registries, trust registries, or oracles that serve as one example of a ToIP Supporting System

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"



CEREMONY

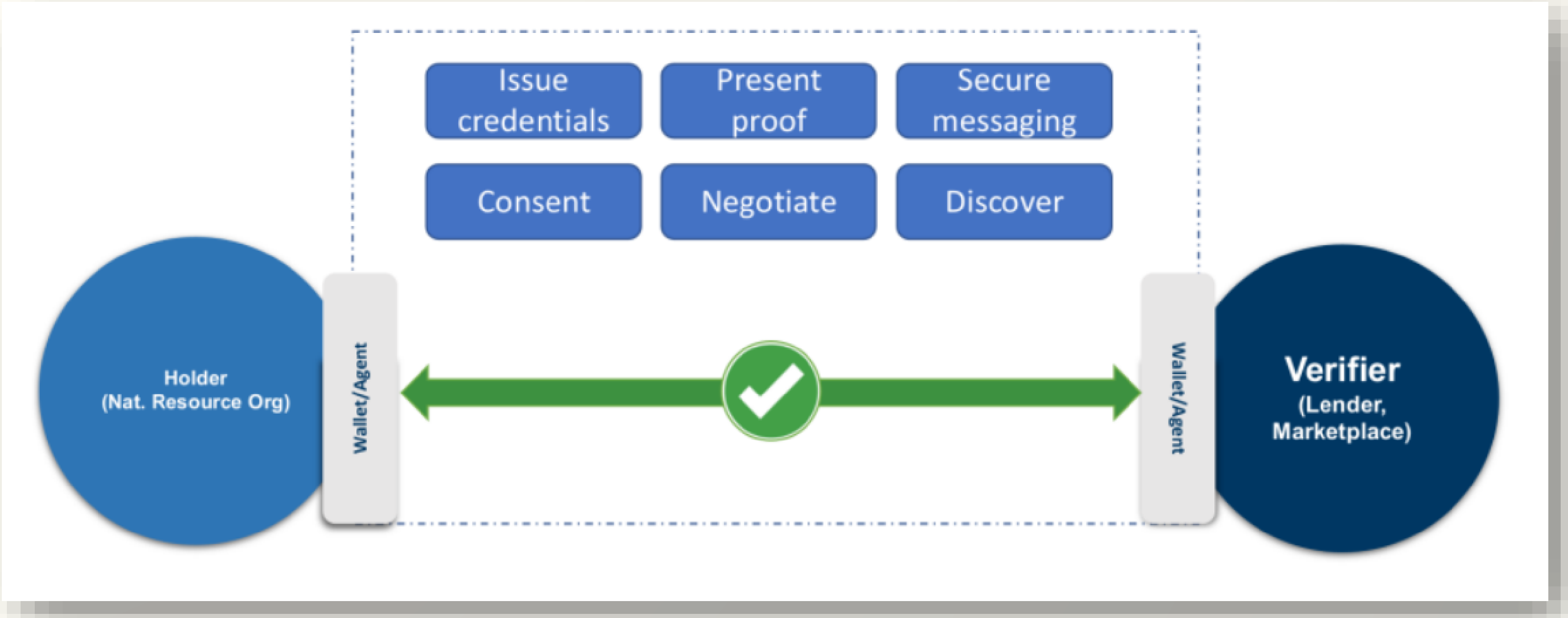
Wallet-to-wallet connections are established and persist until one party opts out.

EXCHANGE

Data wallets interoperate to exchange peer Decentralized IDentifiers (DIDs) and public keys without intermediaries.

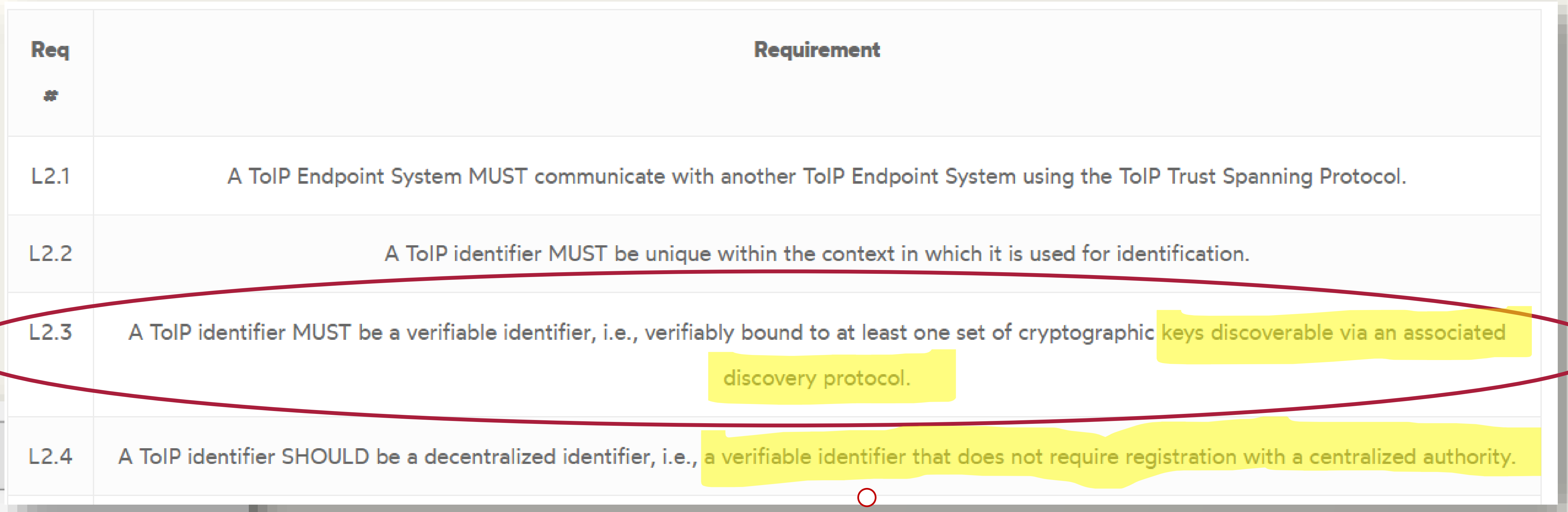
We need to pay attention to development around DIDComm V2 and the impacts on DNS usage

- https://identity.foundation/didcomm-messaging/spec/

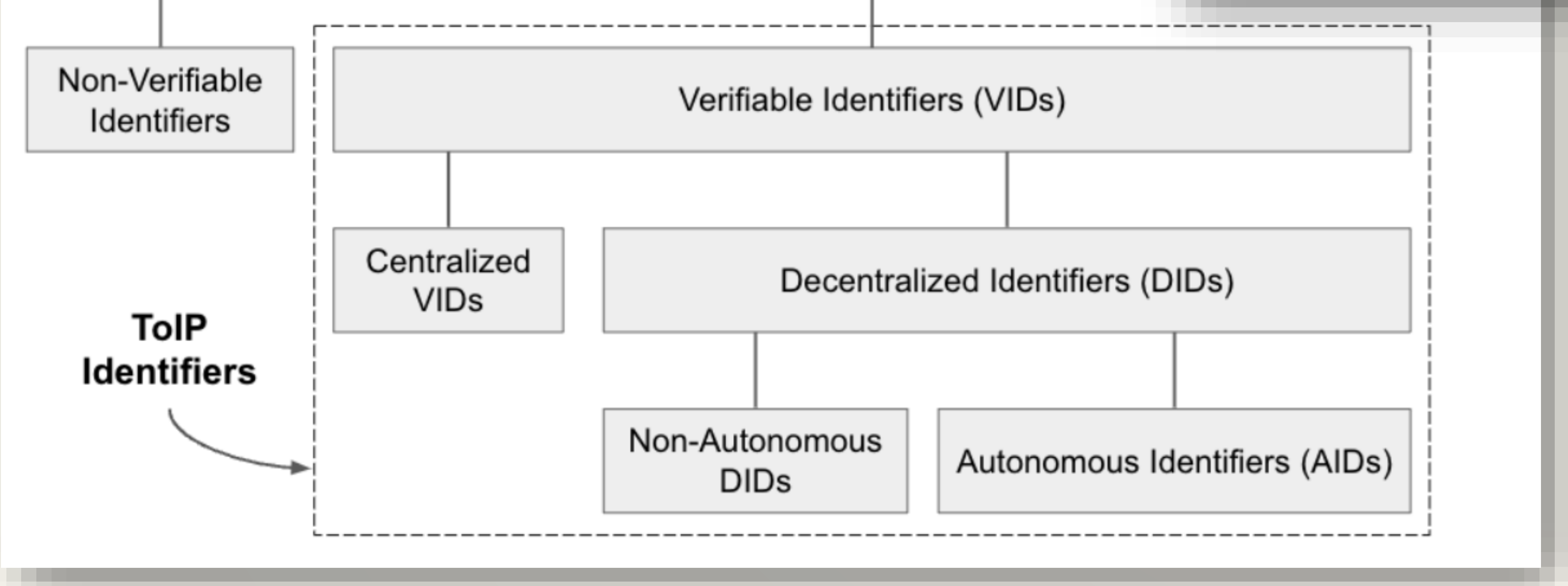


A TRUST LAYER IS EMERGING

Digital Credentials ~= Decentralized and Verifiable Identifiers



Req #	Requirement
L2.1	A ToIP Endpoint System MUST communicate with another ToIP Endpoint System using the ToIP Trust Spanning Protocol.
L2.2	A ToIP identifier MUST be unique within the context in which it is used for identification.
L2.3	A ToIP identifier MUST be a verifiable identifier, i.e., verifiably bound to at least one set of cryptographic keys discoverable via an associated discovery protocol.
L2.4	A ToIP identifier SHOULD be a decentralized identifier, i.e., a verifiable identifier that does not require registration with a centralized authority.


All Identifiers
Non-Verifiable Identifiers
Verifiable Identifiers (VIDs)
Centralized VIDs
Decentralized Identifiers (DIDs)
ToIP Identifiers
Non-Autonomous DIDs
Autonomous Identifiers (AIDs)

Trying to get the DNS as a discovery protocol for ToIP identifiers

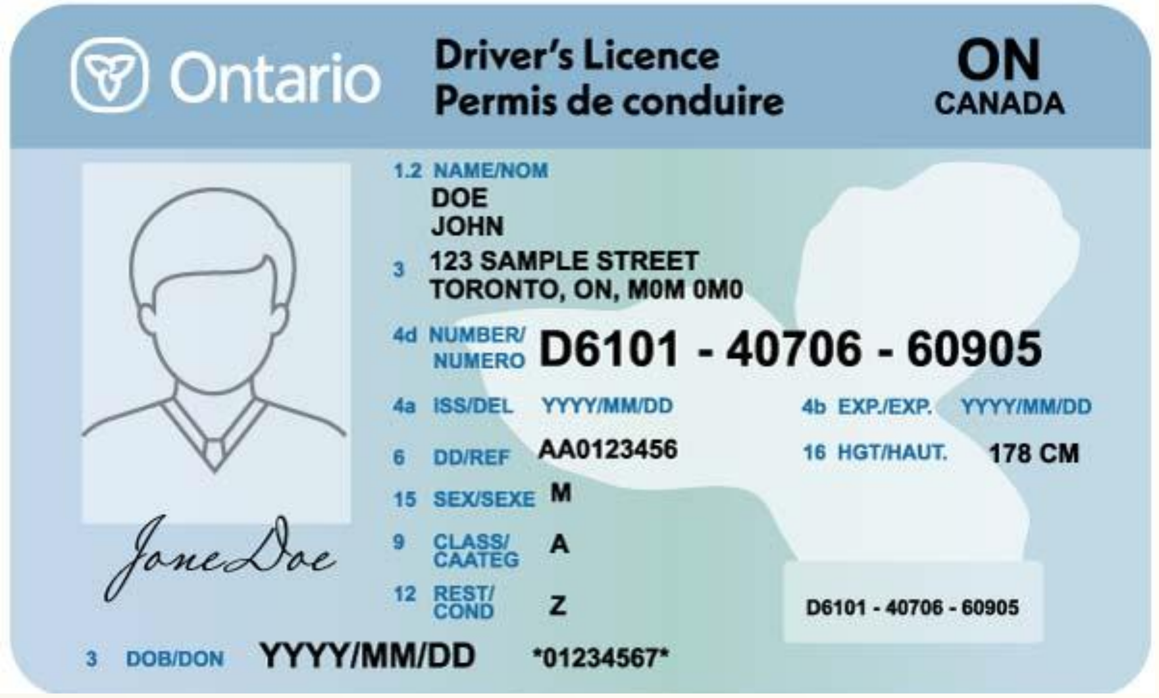
https://www.trustoverip.org/blog/2023/01/05/the-toip-trust-spanning-protocol/

DIGITAL CREDENTIAL DECENTRALIZATION

Example of a digital credentials: A Driver’s license

WWW.CIRA.CA

PLASTIC



Ontario Driver’s Licence Permis de conduire ON CANADA

1.2 NAME/NOM DOE JOHN

3 123 SAMPLE STREET TORONTO, ON, M0M 0M0

4d NUMBER/ NUMERO D6101 - 40706 - 60905

4a ISS/DEL YYYY/MM/DD

4b EXP./EXP. YYYY/MM/DD

6 DD/REF AA0123456

16 HGT/HAUT. 178 CM

15 SEX/SEXE M

9 CLASS/ CAATEG A

12 REST/ COND Z

D6101 - 40706 - 60905

JaneDoe

3 DOB/DON YYYY/MM/DD *01234567*

DIGITAL

```
"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_datete": "1998-08-28“
        "issuing_countryry": “CA”
        "issuing_authorityty": “ON",
"proof":
     "type": "Ed25519Signature2020",
     "verificationMethod": "did:key:z6Mkjxv…Fgy2E5#key1“ (public key)
     "proofValue": "z4zKSH1WmuSQ8tcpS…FaiLvBUjJ89GP7V" (signature)
```

cira

CLASSIFICATION:PUBLIC

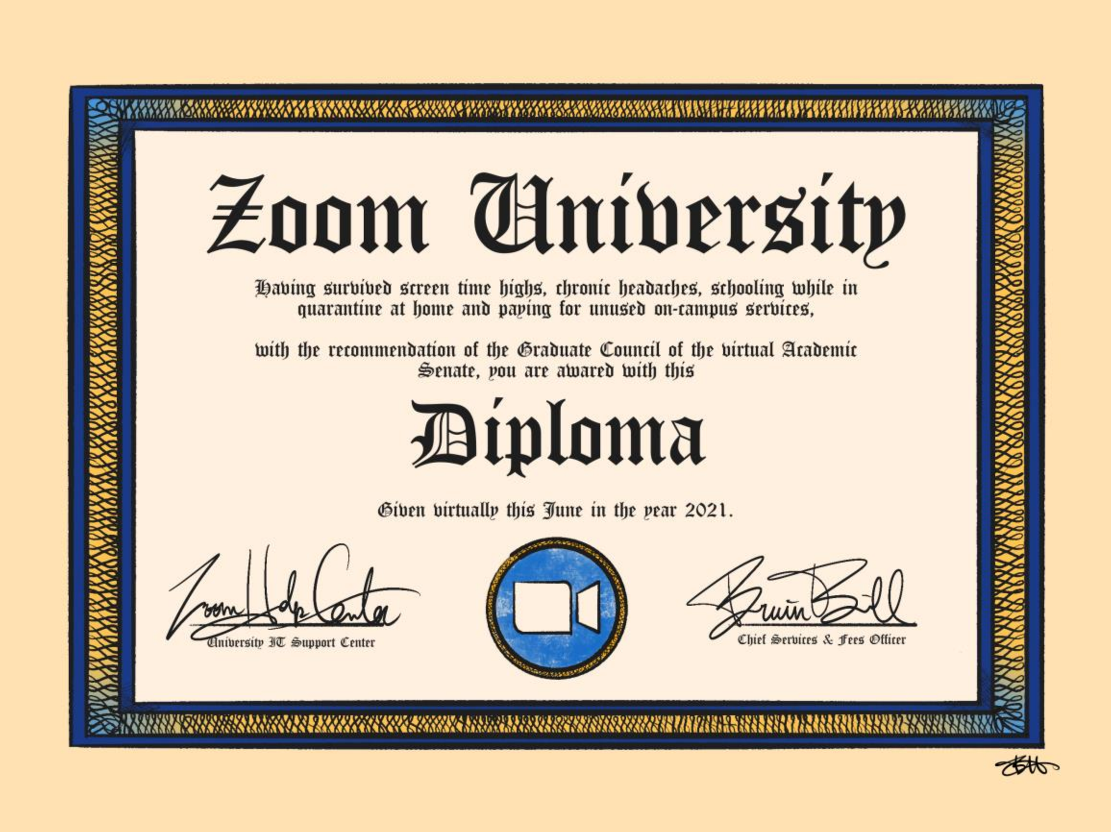
Example of a decentralized Identifier (DID): Driver’s licenses issuer

```
"@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": "HdXo5kegxgPze3tAw6QY...sB6eS"
     }
 ]
"authentication": ["did:key:z6Mkjxv…Fgy2E5#key1"]
"assertionMethod": ["did:key:z6Mkjxv…Fgy2E5#key1"]
```

DIGITAL CREDENTIAL DECENTRALIZATION

Another example of a digital credential

Paper



Zoom University

Having survived screen time highs, chronic headaches, schooling while in quarantine at home and paying for unused on-campus services,

with the recommendation of the Graduate Council of the virtual Academic Senate, you are awared with this

Diploma

Given virtually this June in the year 2021.

Zoom Help Center
University IT Support Center

Bruin Bill
Chief Services & Fees Officer

DIGITAL

```
"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 needs 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