Interop Profiles, Oh My

A Trust Registry Protocol Proposal

Andor Kessleman
(Benri)

Disclaimer: This is meant to start ideation, but it will be rough in a quite a few areas.

Protocol Proposal

- Literature Review
- Assertions
- Modeling and Problem Statement
- Design Principles
- Proposal
- Ecosystem
- Code
- Conclusion/Discussion

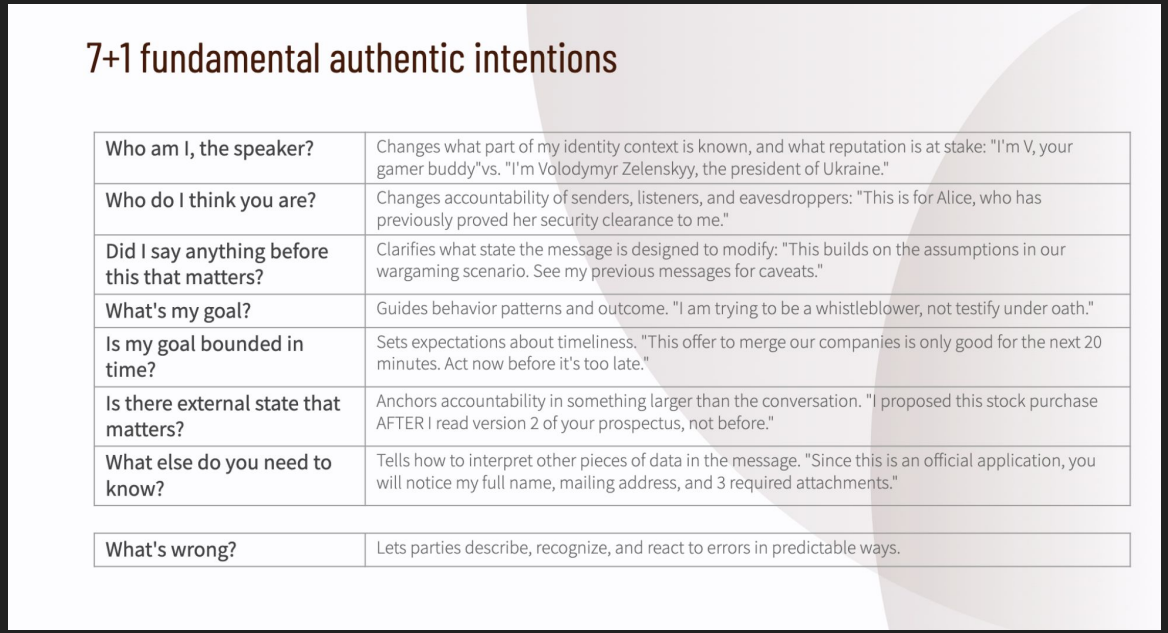
Literature Review

Requirements Document

- Requirements Document
  - Existing Trust Registries
    - EU TRAIN
    - EU Trust Lists
    - DIACC Trust Registry
    - Cira Trust Registry
    - AAMVA mDL
    - Education (Ethiopia)
    - Technical Specification for Digital Credentials and Digital Trust Services
- Transport Agnostic
- Chaining
- Stack Compatible
- Temporal Limitations
- Traceability

Daniel Hardman’s TSP Proposal

- 7+1 fundamental authentic intentions



7+1 fundamental authentic intentions

Who am I, the speaker?	Changes what part of my identity context is known, and what reputation is at stake: "I'm V, your gamer buddy"vs. "I'm Volodymyr Zelenskyy, the president of Ukraine."
Who do I think you are?	Changes accountability of senders, listeners, and eavesdroppers: "This is for Alice, who has previously proved her security clearance to me."
Did I say anything before this that matters?	Clarifies what state the message is designed to modify: "This builds on the assumptions in our wargaming scenario. See my previous messages for caveats."
What's my goal?	Guides behavior patterns and outcome. "I am trying to be a whistleblower, not testify under oath."
Is my goal bounded in time?	Sets expectations about timeliness. "This offer to merge our companies is only good for the next 20 minutes. Act now before it's too late."
Is there external state that matters?	Anchors accountability in something larger than the conversation. "I proposed this stock purchase AFTER I read version 2 of your prospectus, not before."
What else do you need to know?	Tells how to interpret other pieces of data in the message. "Since this is an official application, you will notice my full name, mailing address, and 3 required attachments."

What's wrong?	Lets parties describe, recognize, and react to errors in predictable ways.

Assertions

Assertion A.0

Everyone is an adversary

Assertion A.1

Trust varies with context.

Assertion A.2

The data model of a TR can be abstracted to a trust graph.

Assertion A.3

Trust can be decomposed to reputational and attributional trust

Assertion A.4

A query against a trust registry is an query against a trust graph.

Assertion A.4.1

A query against a reputation system is also a query against a trust graph.

Assertion A.4.2

Trust Registries and reputation systems are it’s congruent technology

Assertion A.5

There exists a sufficiently general protocol that can define a interactions against an trust graph for most contexts.

Assertion A.6

In considering adoption, a simple and more general framework is preferred to a simple and narrow framework.

Assertion A.7

All use cases of adoption are impossible to predict.

Adoption is impacted by unknown systems due to Metcalfe's law.

Trust Decision Modeling

What is a trust decision?

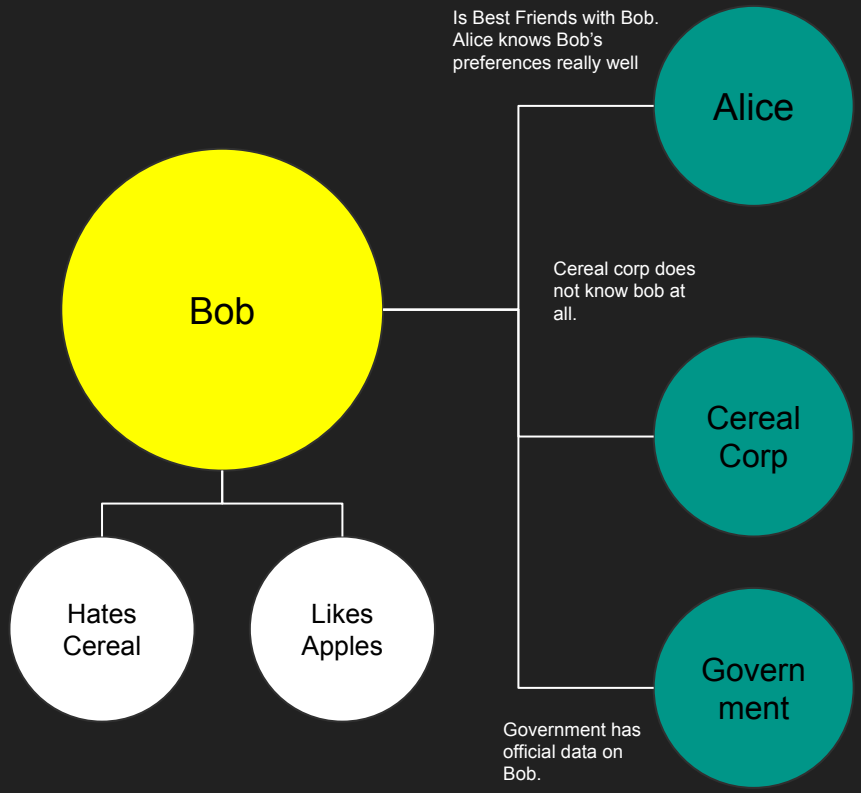
$h(g(f(C, x)))$

- where:
  - $f(C, x)$ is a trust embedding (Trust decision framework mapping)
  - $g(f(C, x))$ is a trust decision
  - $h(g(f(C, x))) = z$ represents an action (or effect) based upon a trust decision. It chooses $z_i \in \mathbb{Z}$ where $\mathbb{Z}$ represents a set of possible effects from a trust decision.
  - C is the decision context
  - x is the set of claims

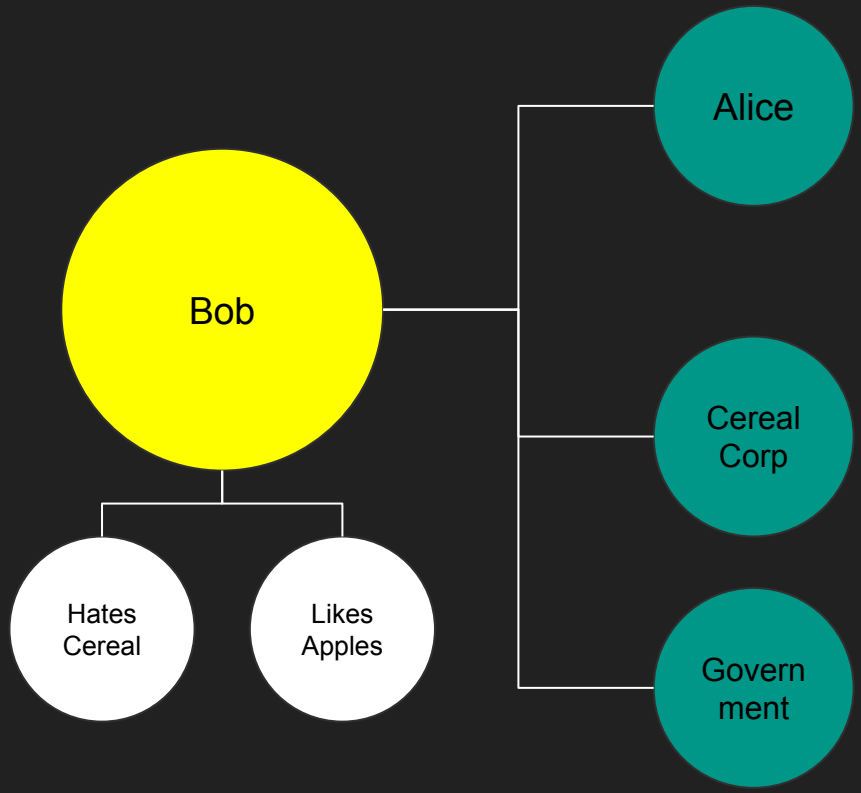
The Bad Cereal

A toy example

Bob is connected to three actors



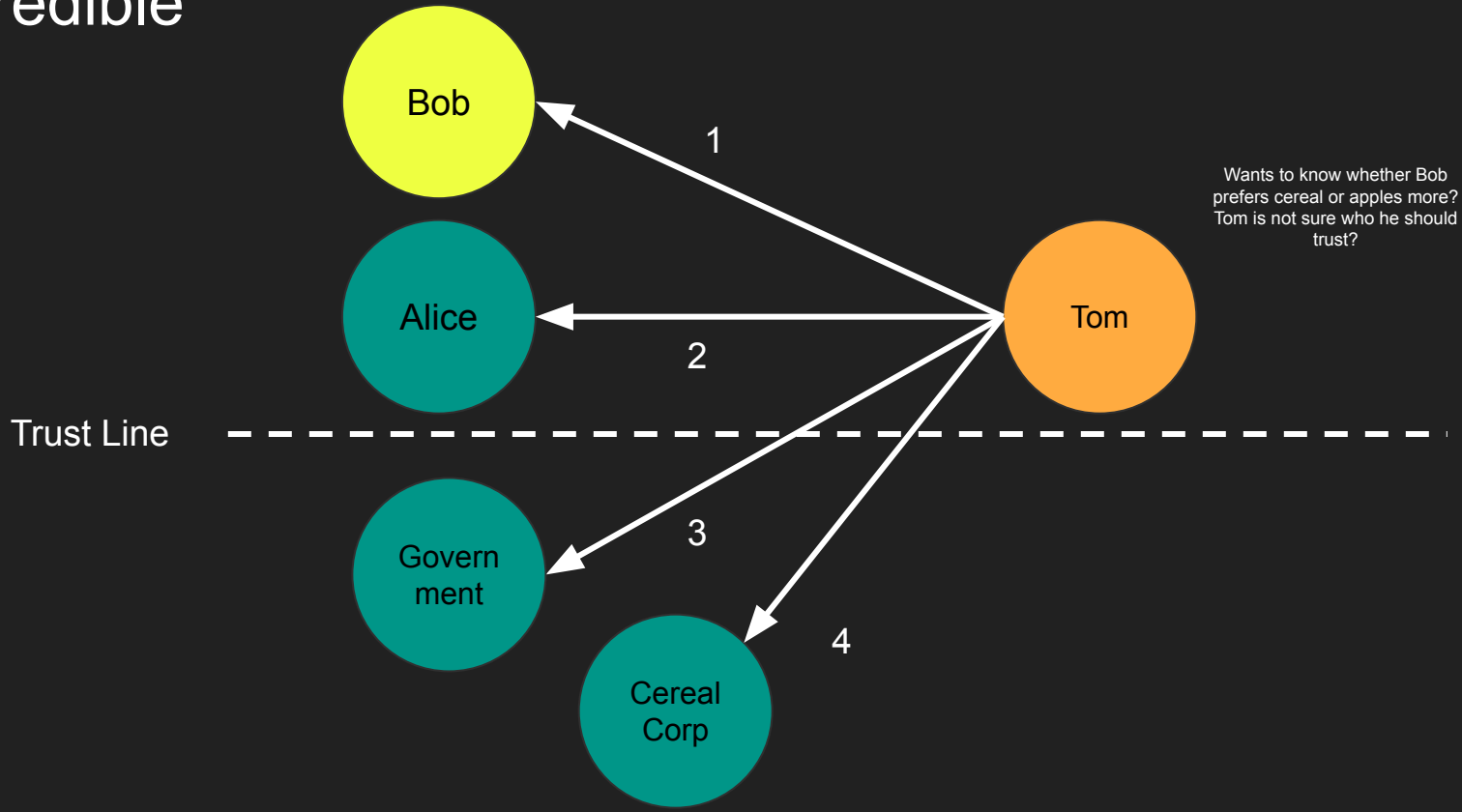
Bob is connected to three actors



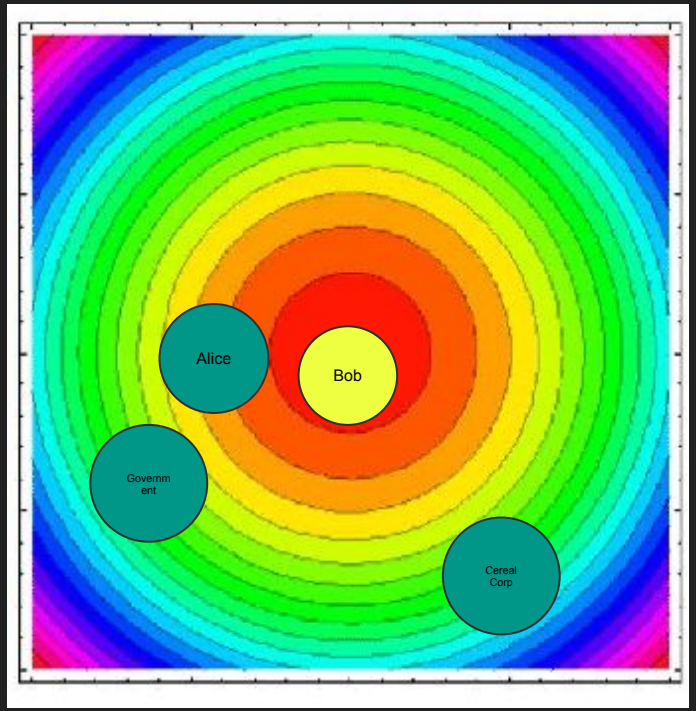
Tom

Wants to know whether Bob prefers cereal or apples more? Tom is not sure who he should trust?

In the context of Bob's food preference, Bob is most credible



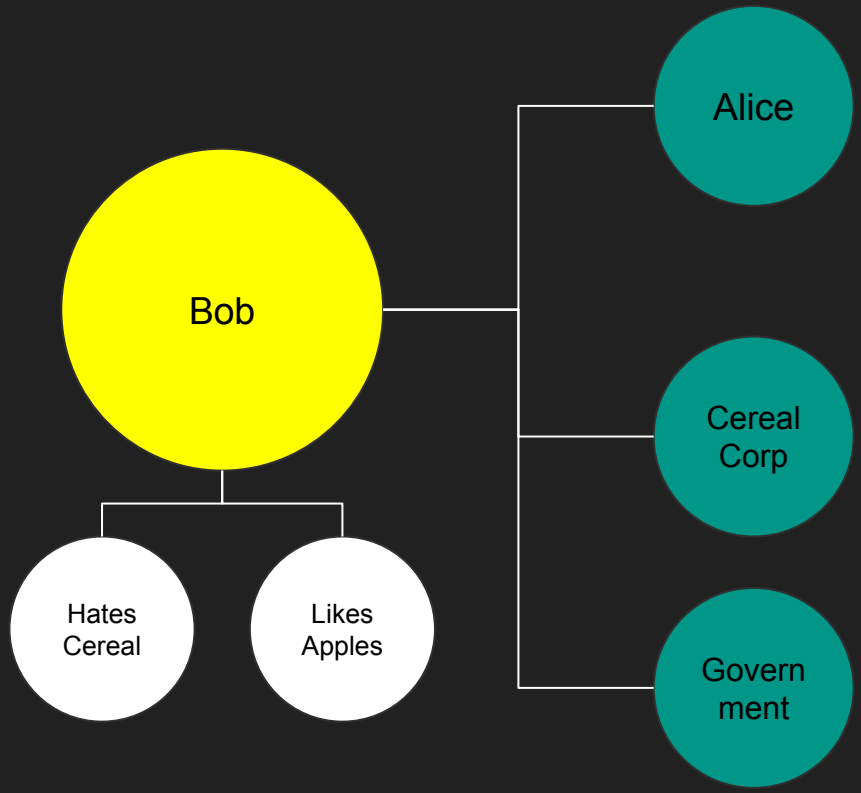
Food Preference Trust Embedding



Tom

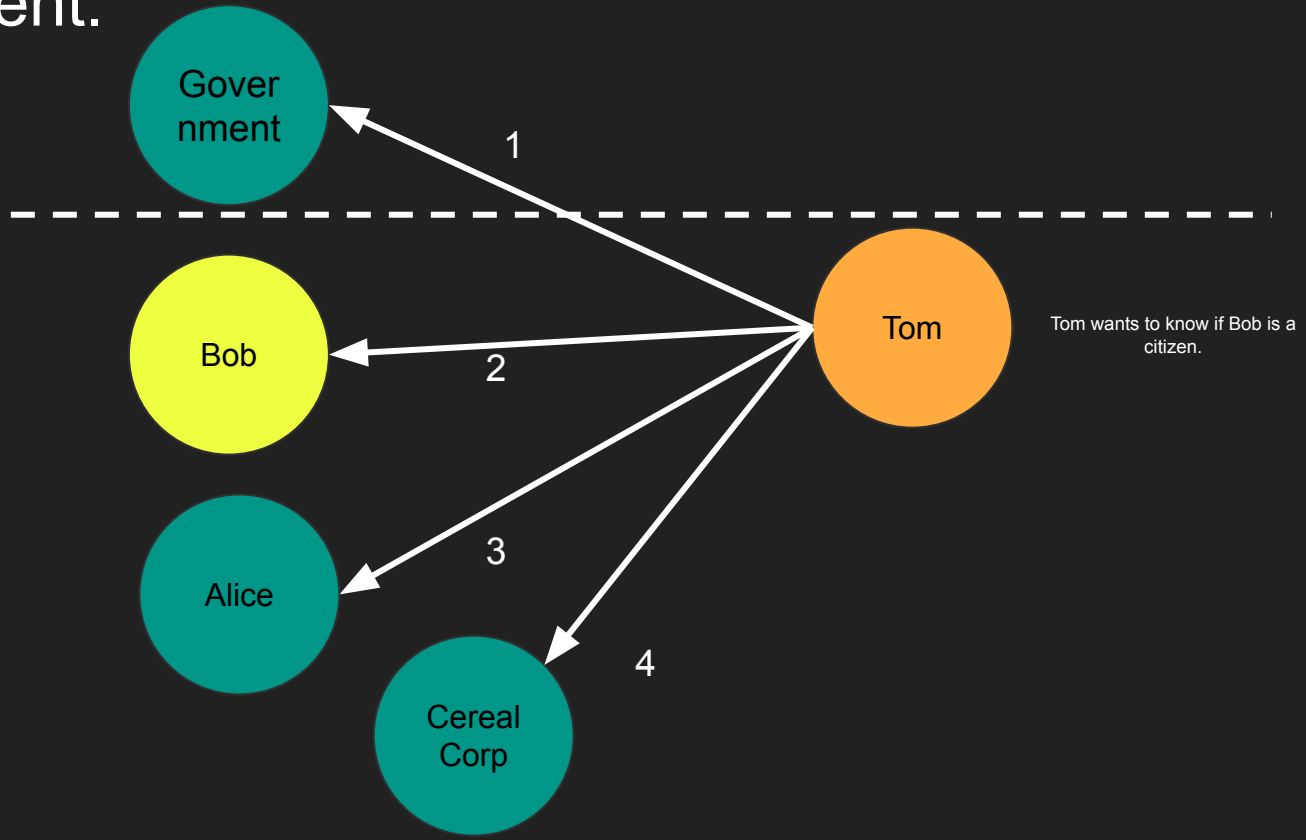
Wants to know whether Bob prefers cereal or apples more? Tom is not sure who he should trust?

Let’s swap the story to citizenship?

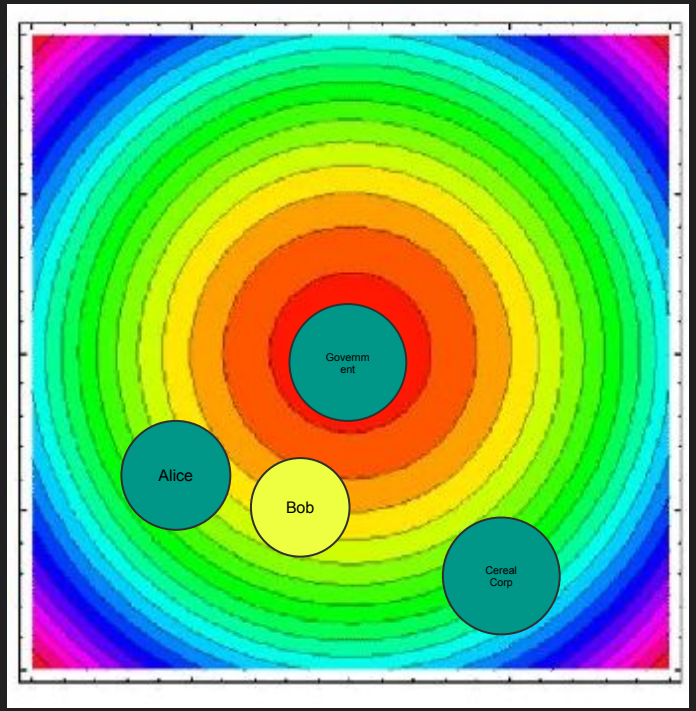


Tom wants to know if Bob is a citizen.

In the context of citizenship, only one source is valid: The government.



Citizen Trust Embedding



Tom

Is Bob a Citizen?

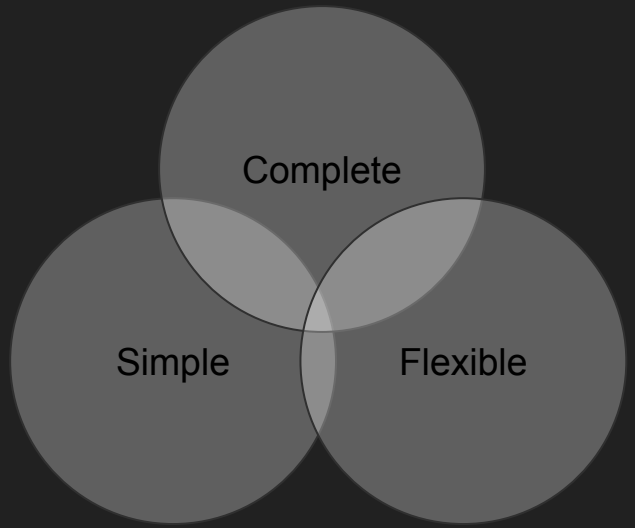
Takeaways

- Context is incredibly important in trust decision making
- Use cases can vary tremendously, from official documents to preferences.
- Bad actors will try to claim things that they will not have credibility to do
- A person’s “decision boundary” changes by preference

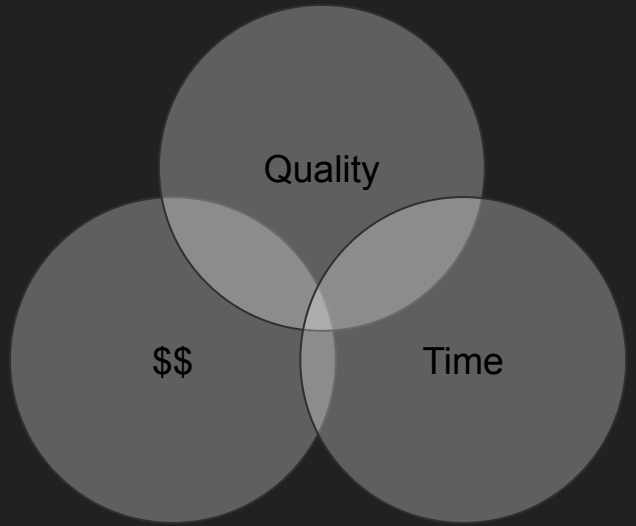
Design Principles

Design Principles

- Simplicity over completeness.
  - Simplicity lends itself well to adoption goals.
- Tightly scoped.
- Flexible design patterns, with expectations of convergence



3 Attributes for the Protocol



Minimization Principles for an Implementation

Proposal

Warning: Lots of things I will declare out of scope

OUT OF SCOPE

- Security WILL be out of scope (i'll explain why later)
- Transports WILL be out of scope. (i'll explain why later)
- Governance WILL be out of scope. (i'll explain why later)
- How to run a TR will be out of scope. (i'll explain why later)
- Building a context will be out of scope. (i'll explain why later)

Step 1: Normative: Add capabilities profile flag to the W3C DID Core Data Model Service Endpoint. TR's are referenceable by DID Document.

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://trustoverip.com/ns/did/v1/service"
  ],
  "id": "did:example:123456789abcdefghi",
  "verificationMethod": [
    {
      "id": "did:example:123456789abcdefghi#keys-1",
      "type": "Ed25519VerificationKey2018",
      "controller": "did:example:123456789abcdefghi",
      "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
    }
  ],
  "service": [
    {
      "id": "did:example:123456789abcdefghi#trust-registry",
      "type": "TrustRegistry",
      "profile": ["https://trustoverip/profiles/basic_profile"],
      "serviceEndpoint": "https://tr.example.com/8377464"
    },
    {
      "id": "did:example:123456789abcdefghi#messages",
      "type": "MessagingService",
      "serviceEndpoint": "https://example.com/messages/8377464"
    }
  ]
}
```

Step 2: Normative Define Profile

Profiles provide metadata on “capabilities” of profile.

Profile is a JSON-LD document.

The following components are defined:

- Name of the profile
- Allowable transports
- Version
- Operations w/ Metadata
- Contexts
- Defines “data contract”
- Defines exchange protocol

TODO: Define CORE mapping.

```
"title": "DID List Profile",
"allowable_transports": ["http", "https"],
"verison": "v0.0.1",
"operations_supported": {
  "query": {
    "document": {
      "get": {
        "comment": "A list of DIDs",
        "@id": "did:sov:123456789abcdefghi1234;spec/did-list/0.0.1/get",
        "supported_content_types": ["application/json"],
        "supported_query_parameters": [
          "type",
          "id",
          "issuer",
          "subject",
          "recipient",
          "label"
```

```
{
  "@context": {
    "title": "http://schema.org/title",
    "allowable_transports": {
      "@id": "https://trustoverip.com/context/profiles/v1/allowable_transports",
      "@type": "@id"
    },
    "version": {
      "@id": "https://trustoverip.com/context/profiles/v1/version",
      "@type": "@id"
    },
    "operations_supported": {
      "@id": "https://trustoverip.com/context/profiles/v1/operations_supported",
      "@type": "@id",
      "@context": {
        "query": {
          "@id": "https://trustoverip.com/context/profiles/v1/query",
          "@type": "@id"
        }
      }
    }
  }
}
```

Step 3: Provide Standard Data Model Container For Additional Assurances

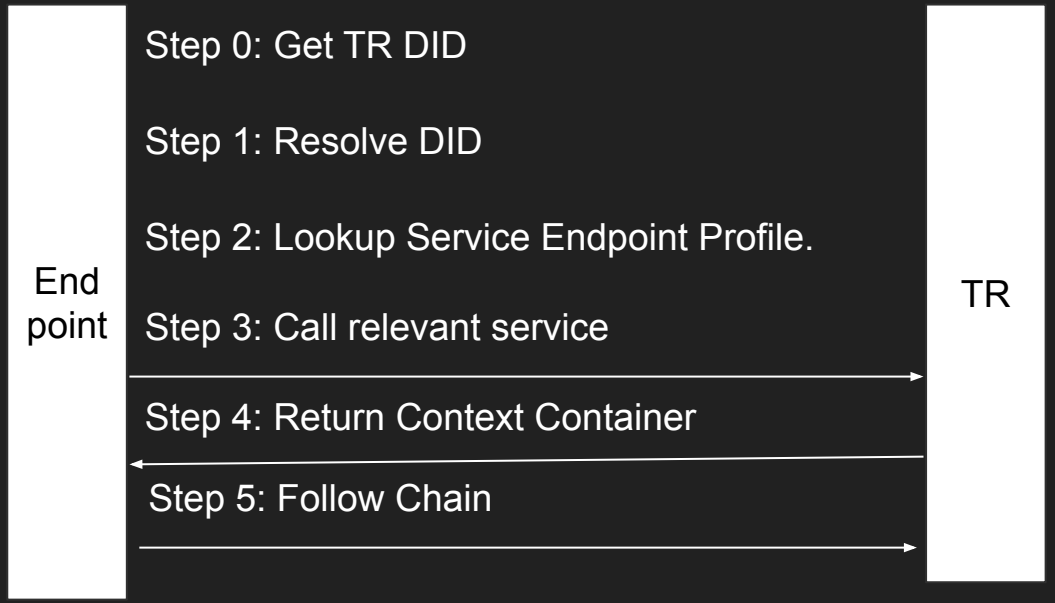
Container for providing reputational and attributional context for response.

Two required fields:

- Data
- Context

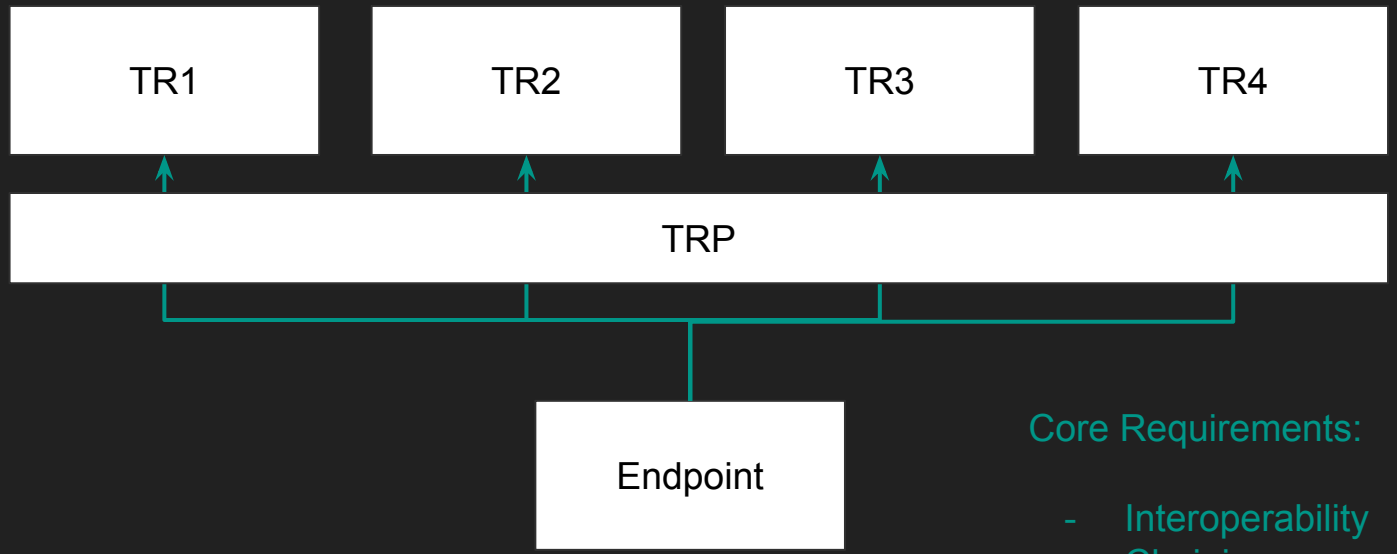
All others are optional

Flow


End point
Step 0: Get TR DID
Step 1: Resolve DID
Step 2: Lookup Service Endpoint Profile.
Step 3: Call relevant service
Step 4: Return Context Container
Step 5: Follow Chain
TR

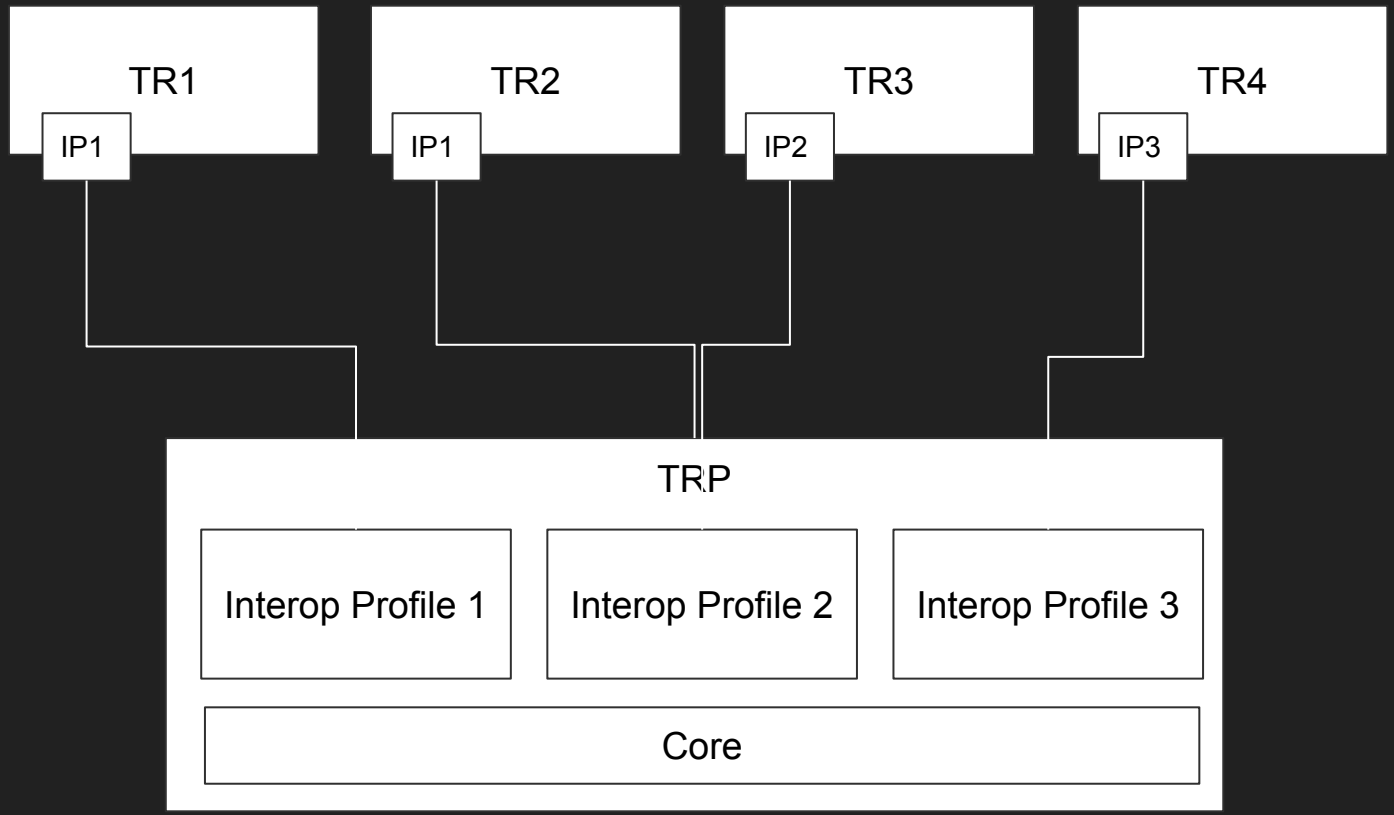
Ecosystem

Modeling the TRP



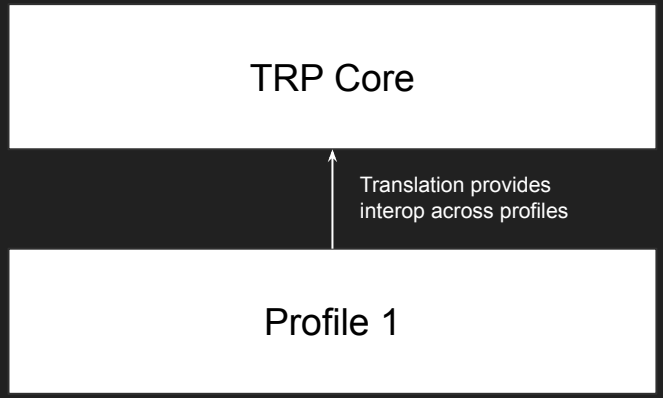
Core Requirements:

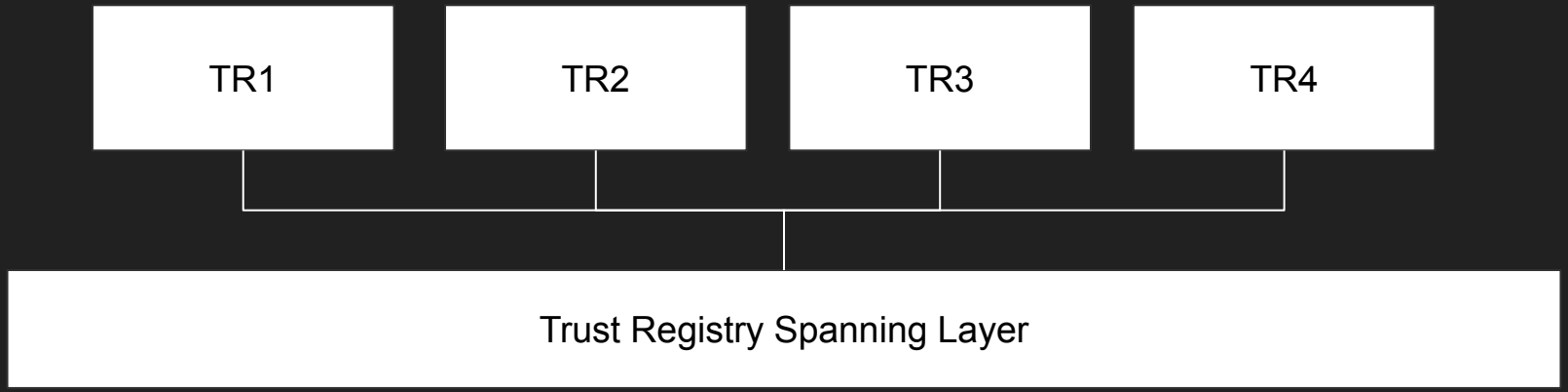
- Interoperability
- Chaining
- Equivalence


TR1
IP1
TR2
IP1
TR3
IP2
TR4
IP3
TRP
Interop Profile 1
Interop Profile 2
Interop Profile 3
Core

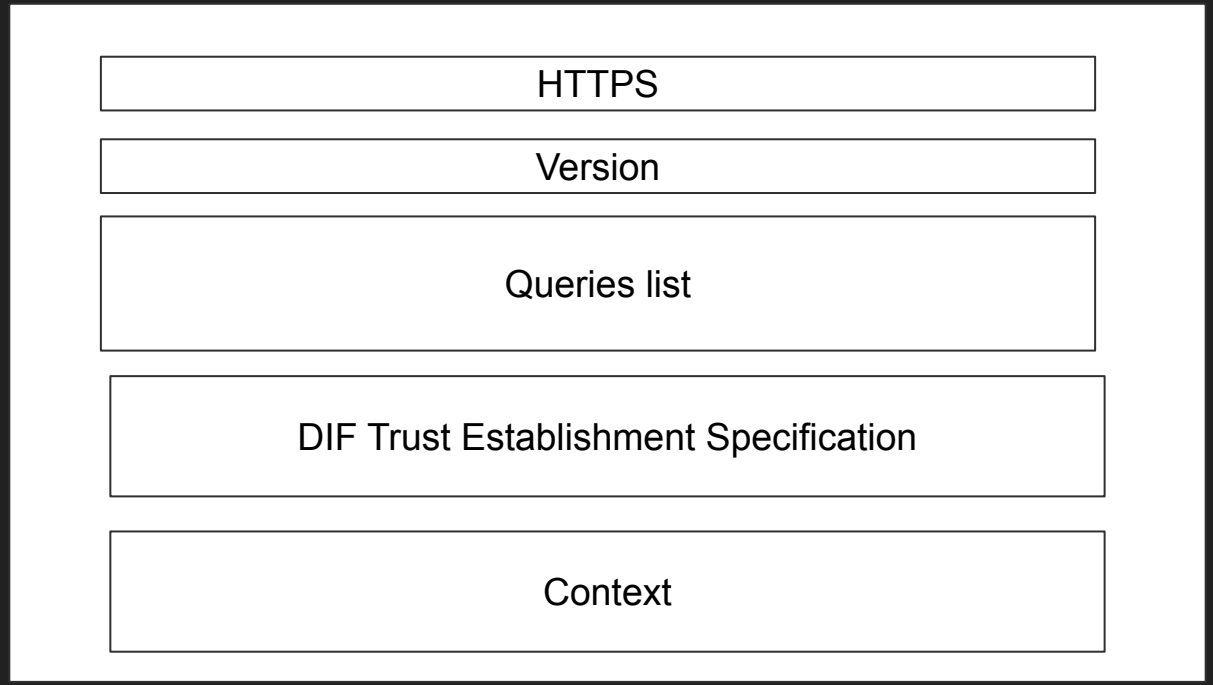
Service Interop

- Intra-profile is natively interoperable
- Inter-profile requires transformer. For each profile, a mapping between a profile and core objects should be provided



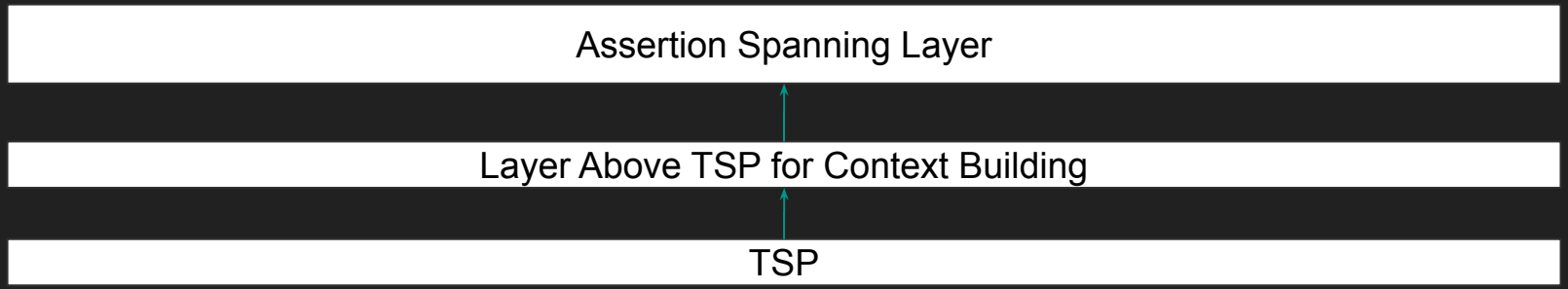

TR1
TR2
TR3
TR4
Trust Registry Spanning Layer

DIF Interop HTTPS Profile



TSP

Additional context can be provided by the TSP and layers above. TR can require context for requests, if needed.



What is a trust registry?

A place where records are kept about trusted sources. Usually in a some conceptual list.

Context Container

sr (source identifier)	Required. AID. Gives sender's intent WRT the reputational context for the message.
sig (source identifier)	Required. Signature over header and payload.
a (audience identifiers)	Optional (missing → audience is "any"). Array of AID. Identifies intended plaintext audience, NOT delivery targets for routing or encrypted envelopes.
th (thread)	Optional non-negative 32-bit int. All participants use **sr** + **th** as the thread's lookup key; the sender of a thread's first message must pick a **th** value that makes this combination unique enough for all practical purposes. Groups messages by topic into logically related streams with different goals, states, and trust profiles.
mo (message ordinal)	Required if **th**. Monotonically increasing, non-negative 32-bit int. Counts how many messages sender has previously contributed to this thread; makes gap detectable.
pth (parent thread)	Optional, and only allowed when mo == 0 (starting a new thread). If omitted then, thread is standalone. Otherwise, connects this thread to previous verifiable data.
expiry_time (expiry_time)	Optional. ISO 8601 time format for when the response made by the registry is valid for.
ex (exists)	Optional. Hash with special CESR prefix to clarify PoE type (e.g., blockchain root; IPFS, github commit, build artifact). Proves message was created after the referenced data already existed.
s (message schema)	Required. SAID. Defines structure of rest of payload, including extra headers and attachments.

Modified from Daniel Hardman's TSP Proposal

Service Discovery

- A service MUST be discoverable via DID Core
- Supported APIs are maintained in the ServiceEndpoint section
- Describes profiles but NOT the resources. Resource discovery is INDEPENDENT from service discovery.
    - Not all resources should be discoverable!