



FACTERN

OBJECTS, LINKAGES, EVENTS AND RULES

MAKING AN ATTRIBUTE LINKING WORK

PRIVATE AND CONFIDENTIAL

What makes an attribute useful when it is taken out of context?

 [Value]

What makes an attribute useful when it is taken out of context?

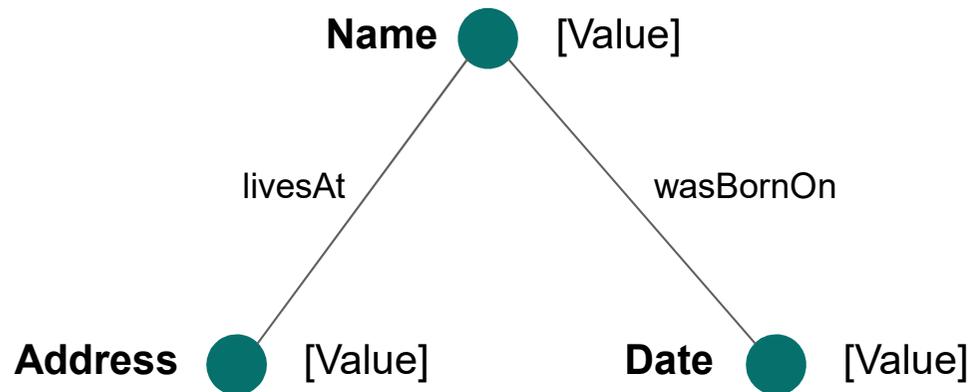
- **Describable**

- What field?
- What format?
- When created?
- Etc.

Name ● [Value]

What makes an attribute useful when it is taken out of context?

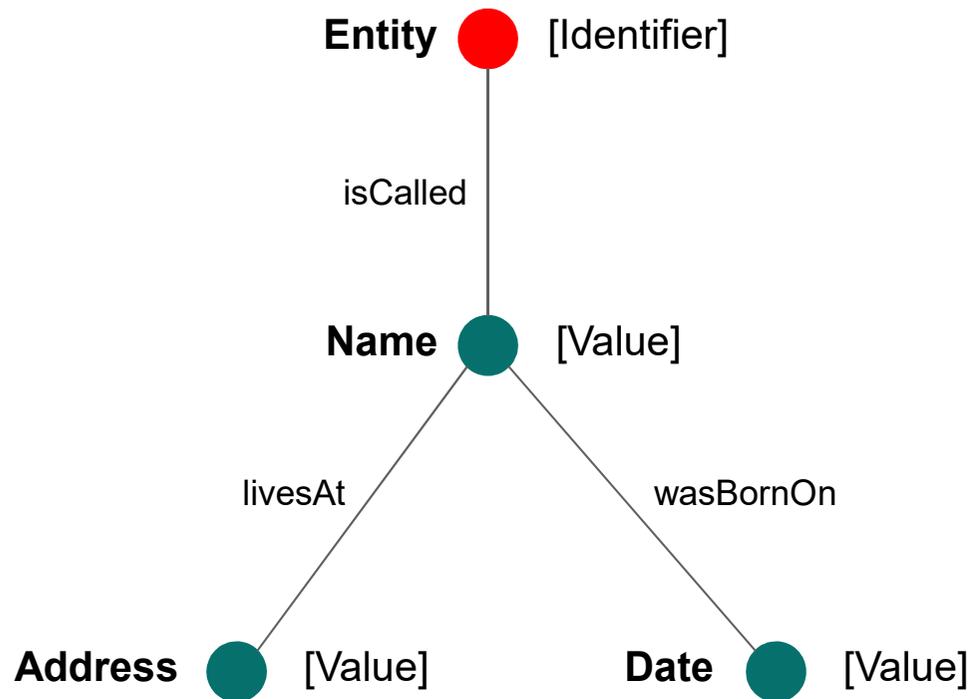
- **Relatable**
 - How does it relate to other attributes?



What makes an attribute useful when it is taken out of context?

- **Relatable**

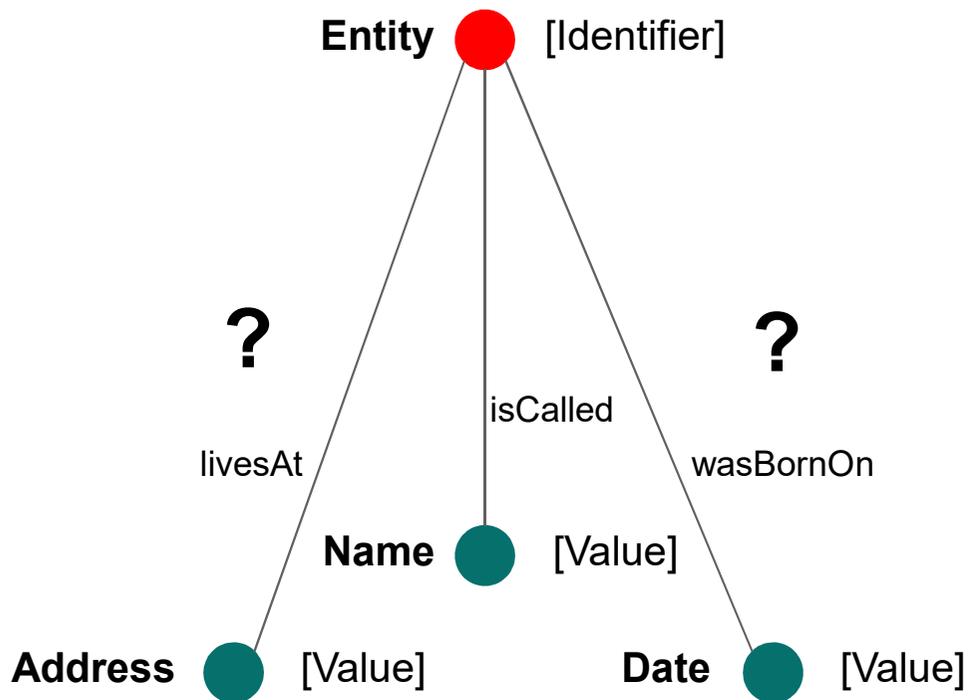
- How does it relate to other attributes?
- What entities is it associated with?



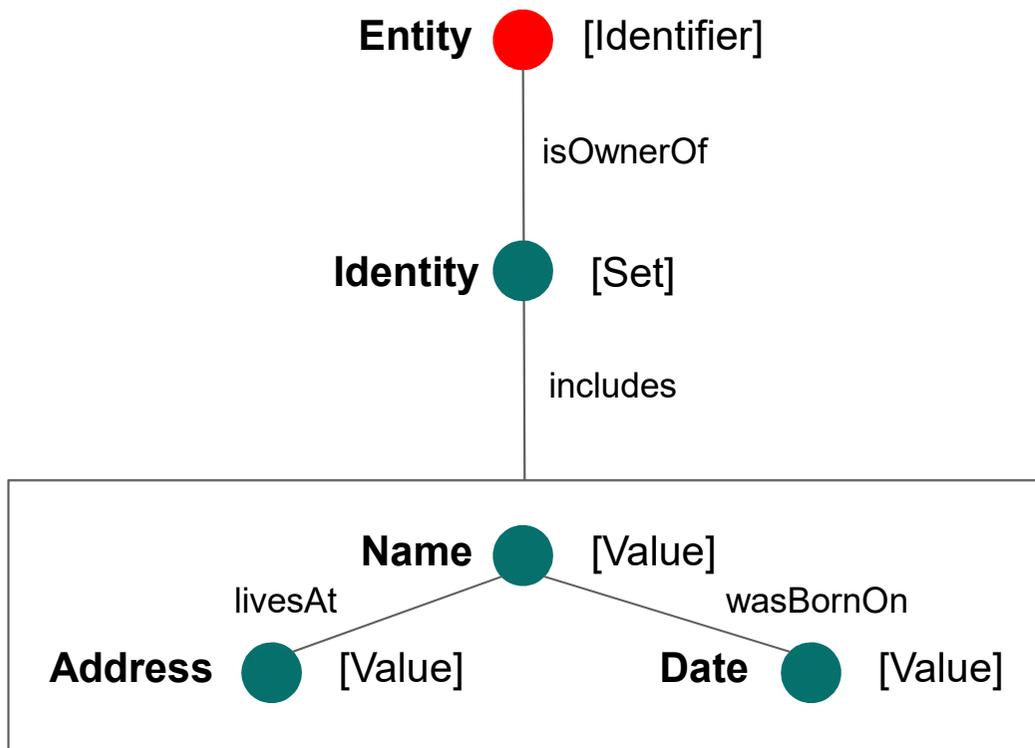
What makes an attribute useful when it is taken out of context?

- **Relatable**

- How does it relate to other attributes?
- What entities is it associated with?
- What can be inferred from this?



What makes an attribute useful when it is taken out of context?



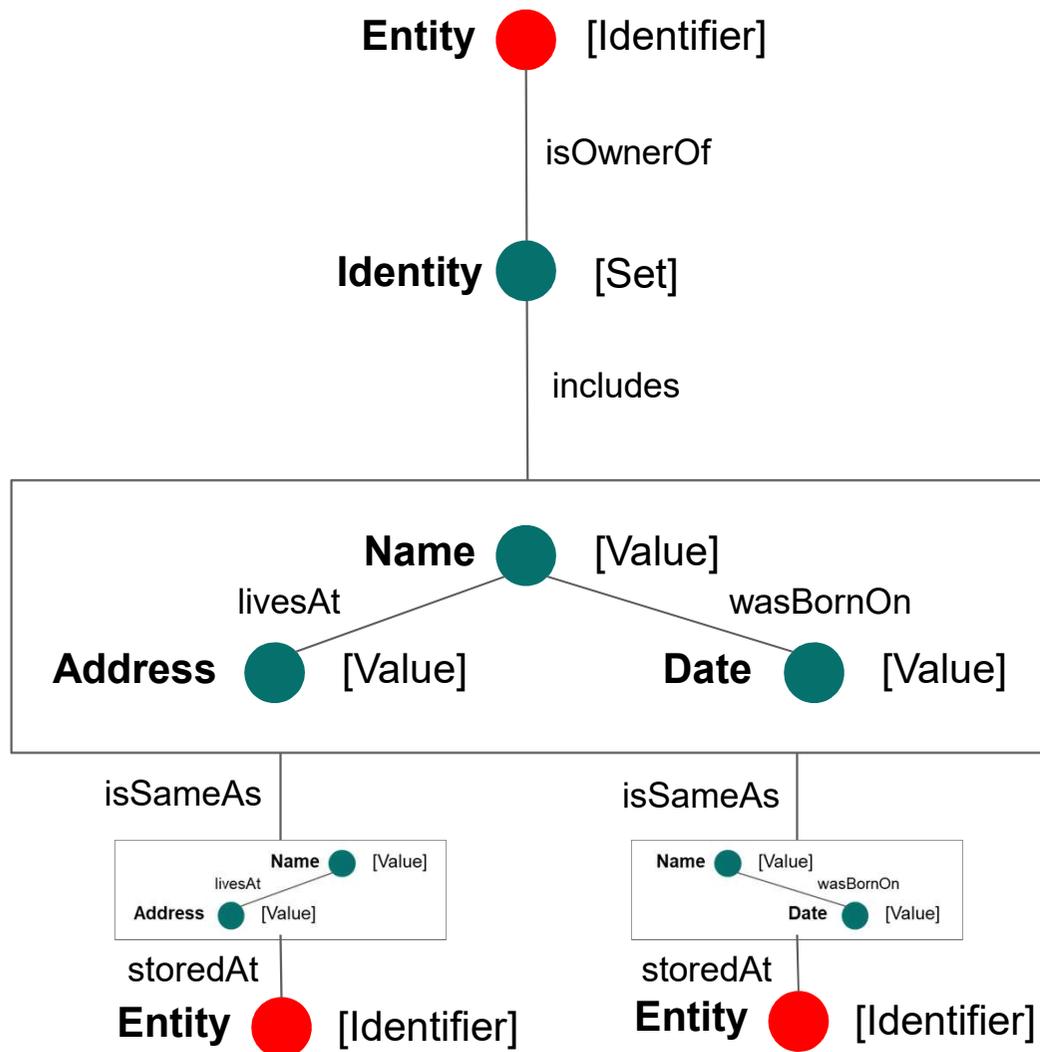
- **Relatable**

- How does it relate to other attributes?
- What entities is it associated with?
- What can be inferred from this?
- Is it part of any sets?

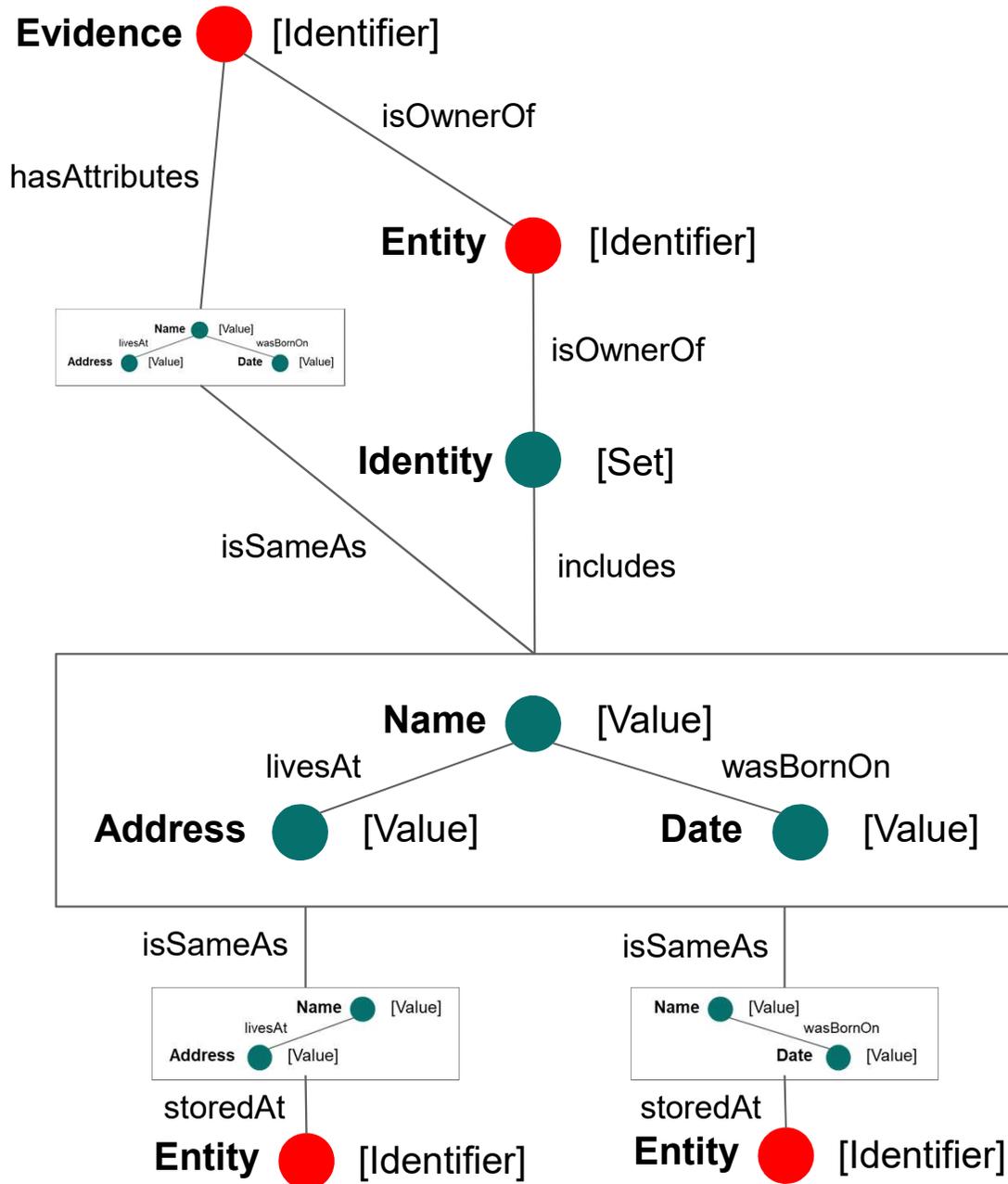
What makes an attribute useful when it is taken out of context?

- **Trustable**

- Can the attribute be corroborated?



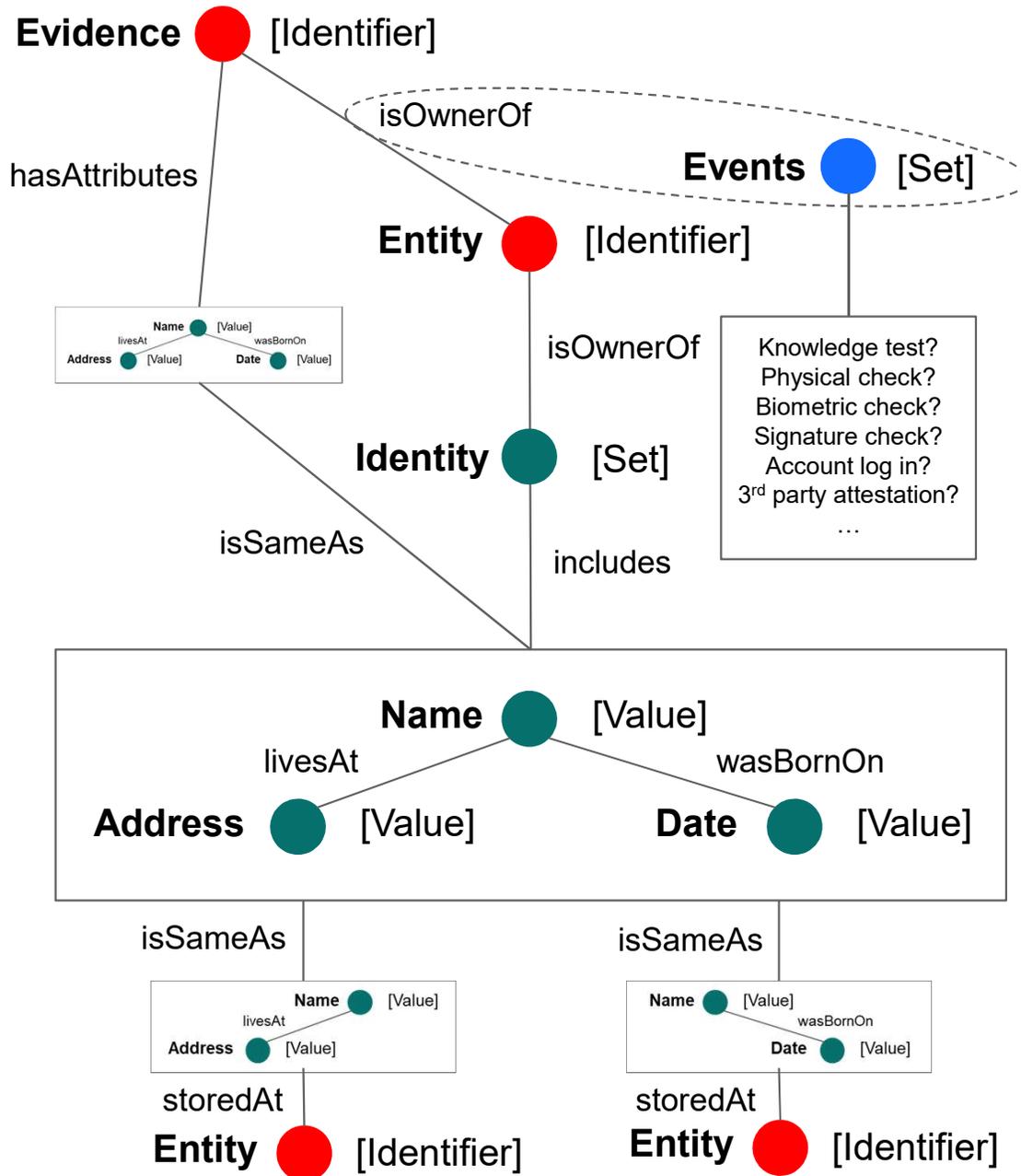
What makes an attribute useful when it is taken out of context?



- **Trustable**

- Can the attribute be corroborated?
- Can the linkages be corroborated?

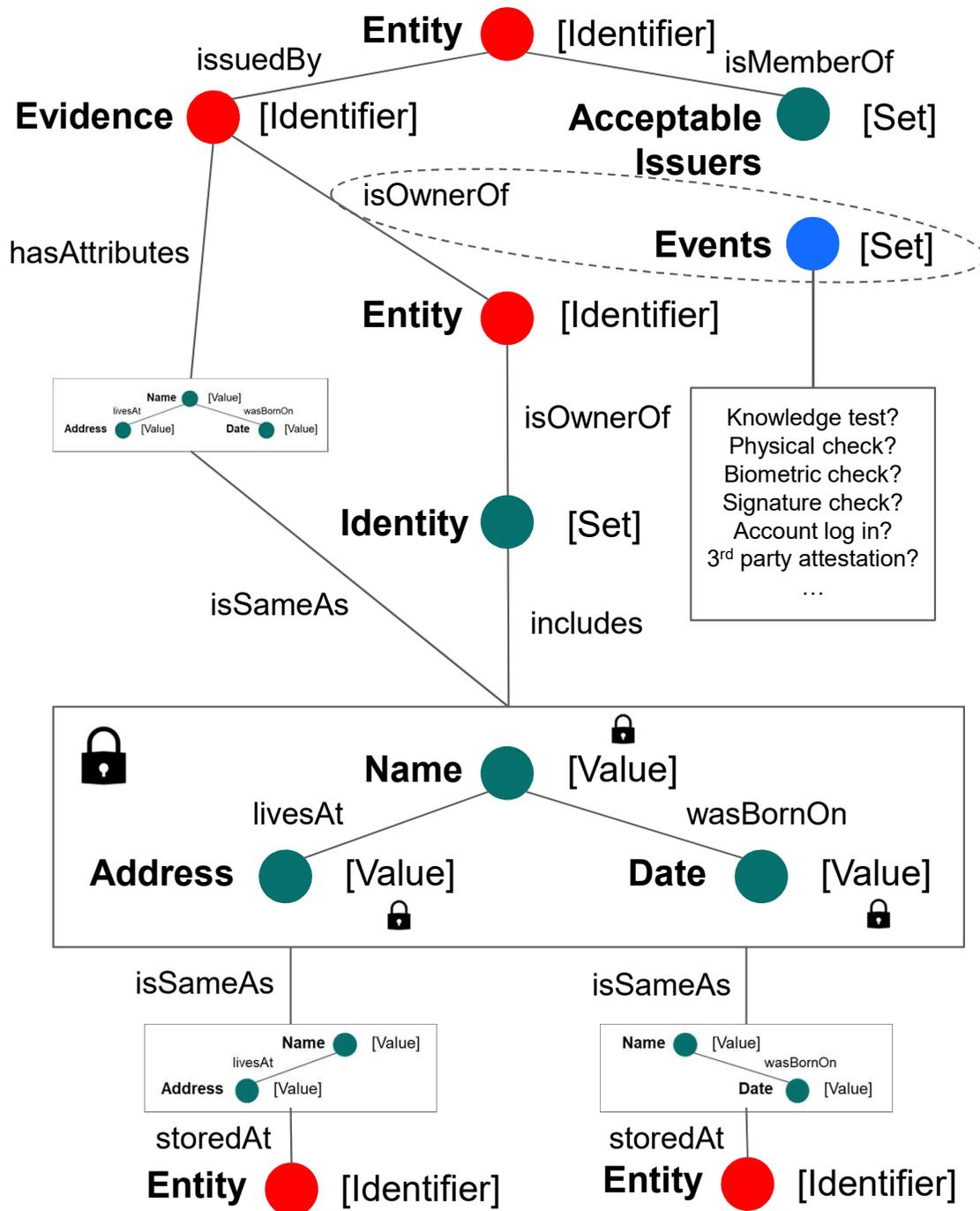
What makes an attribute useful when it is taken out of context?



- **Trustable**

- Can the attribute be corroborated?
- Can the linkages be corroborated?
- What due diligence has been done?
- Who did it?

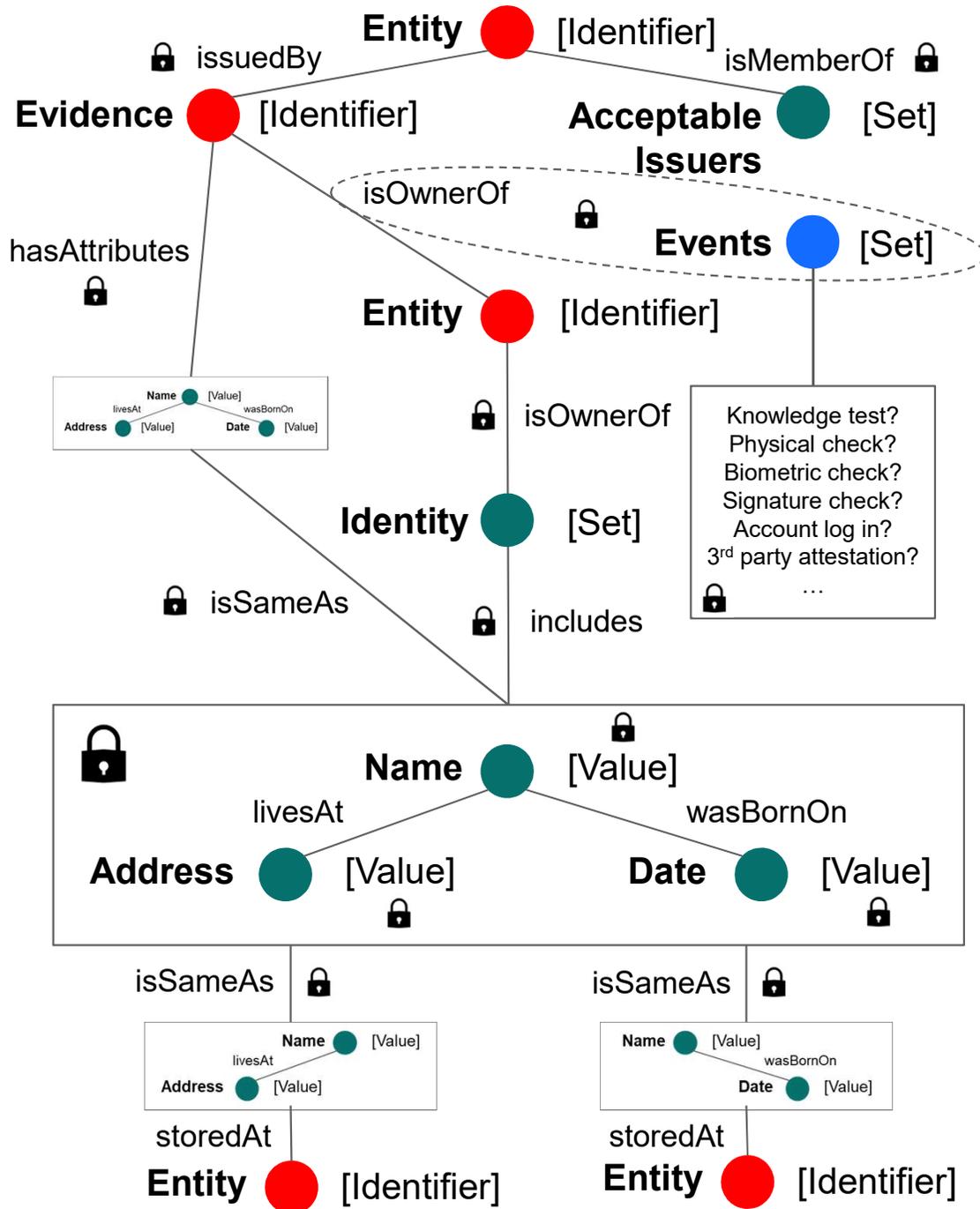
What makes an attribute useful when it is taken out of context?



- **Accessible**

- Where is the attribute stored?
- Who has rights over it?
- What authorisation(s) are needed?
- How are they fulfilled?

What makes an attribute useful when it is taken out of context?



- **Accessible**

- Where is the attribute stored?
- Who has rights over it?
- What authorisation(s) are needed?
- How are they fulfilled?

- **Accessible²**

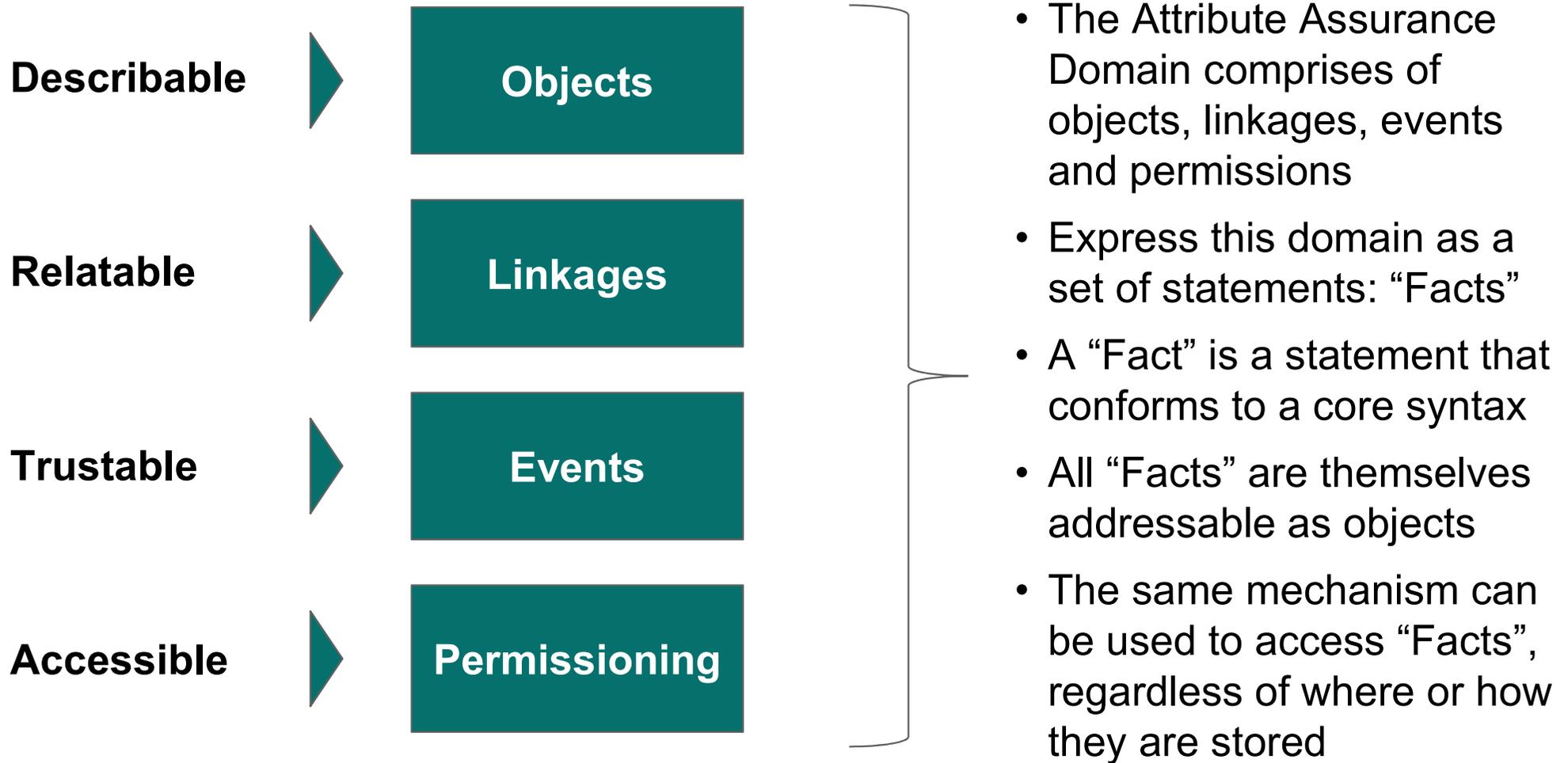
- Where is the *metadata* stored?
- Who has rights over it?
- What authorisation(s) are needed?
- How are they fulfilled?

What makes an attribute useful when it is taken out of context?

Metadata
(lots of it)

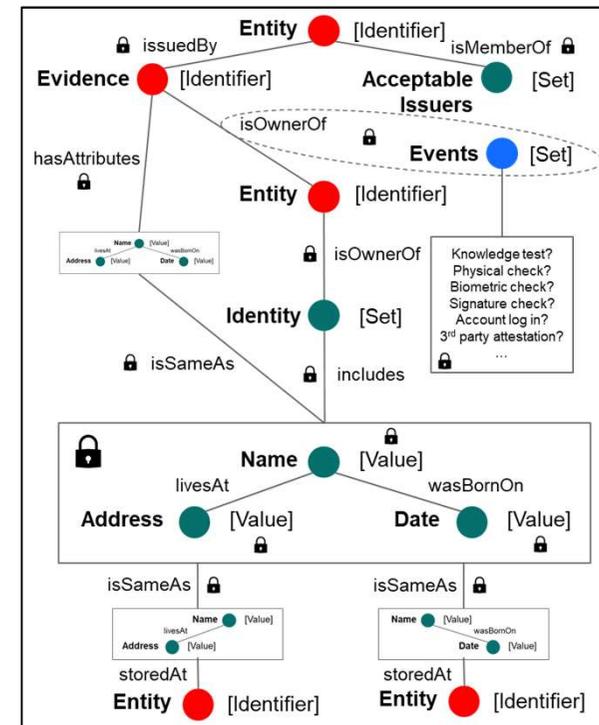
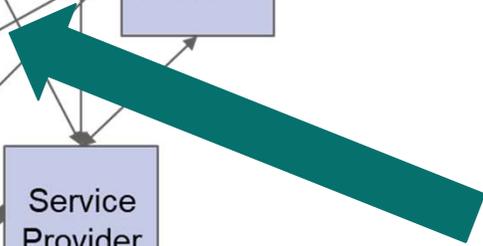
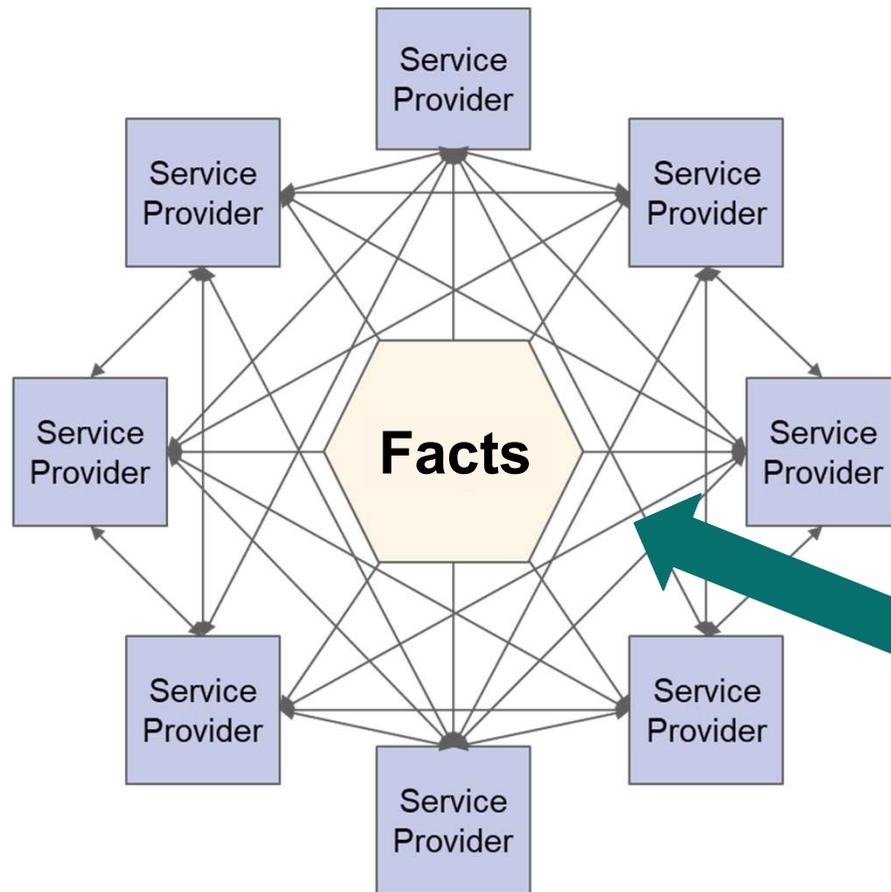
As an ecosystem, we....:

Are interested in objects, linkages, events and permissions



As an ecosystem, we....:

Create a consistent, meaningful and accessible metadata layer



As an ecosystem, we....:

Enforce a consistent syntax; treat all Facts as logically the same

Multiparty “speaker” qualifies how the Fact was authored, to vest trust in the statement itself.

- ◆ Bank employee
 - Manager
 - Supervisor
 - Advisor
 - Trainee
- ◆ Third party
 - Agent
 - Lawyer
 - Accountant
 - Doctor

Used

- ◆ Web-browser app
- ◆ In branch system
- ◆ Paper and pen

To assert that

- ◆ Claimant
- ◆ Customer

- ◆ claimsToHave
- ◆ isInPossessionOf
- ◆ isTheOwnerOf

- ◆ UK Passport
- ◆ UK / EU Driver's Licence
- ◆ EU National ID Card
- ◆ Student Union Card
- ◆ Employee Pass
- ◆ Rail Photocard

Facts can contain information relating to objects, linkages, events or permissions

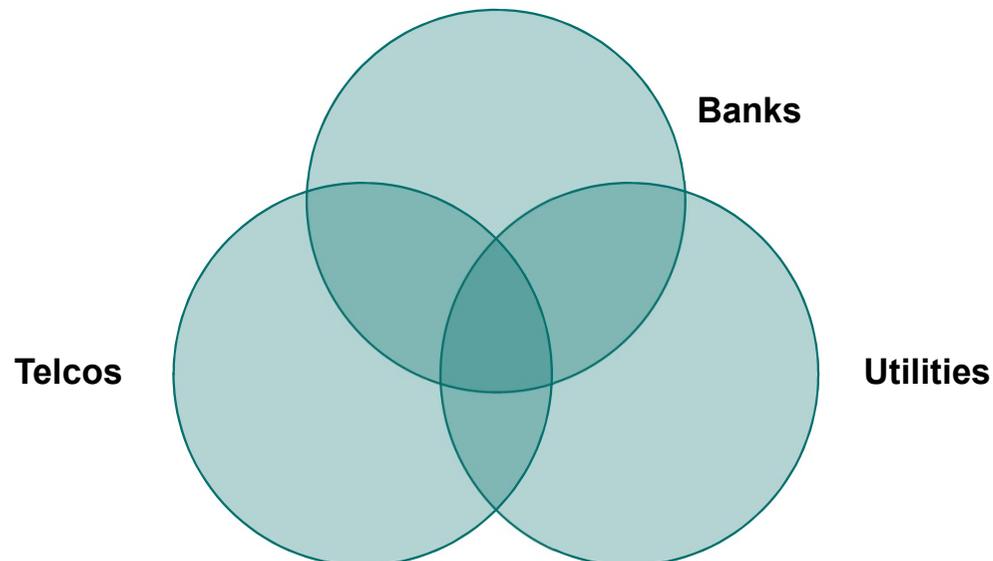
As an ecosystem, we....:

Share vocabularies to make more Facts relevant to each other

Example: events to check evidence belongs to a Claimant

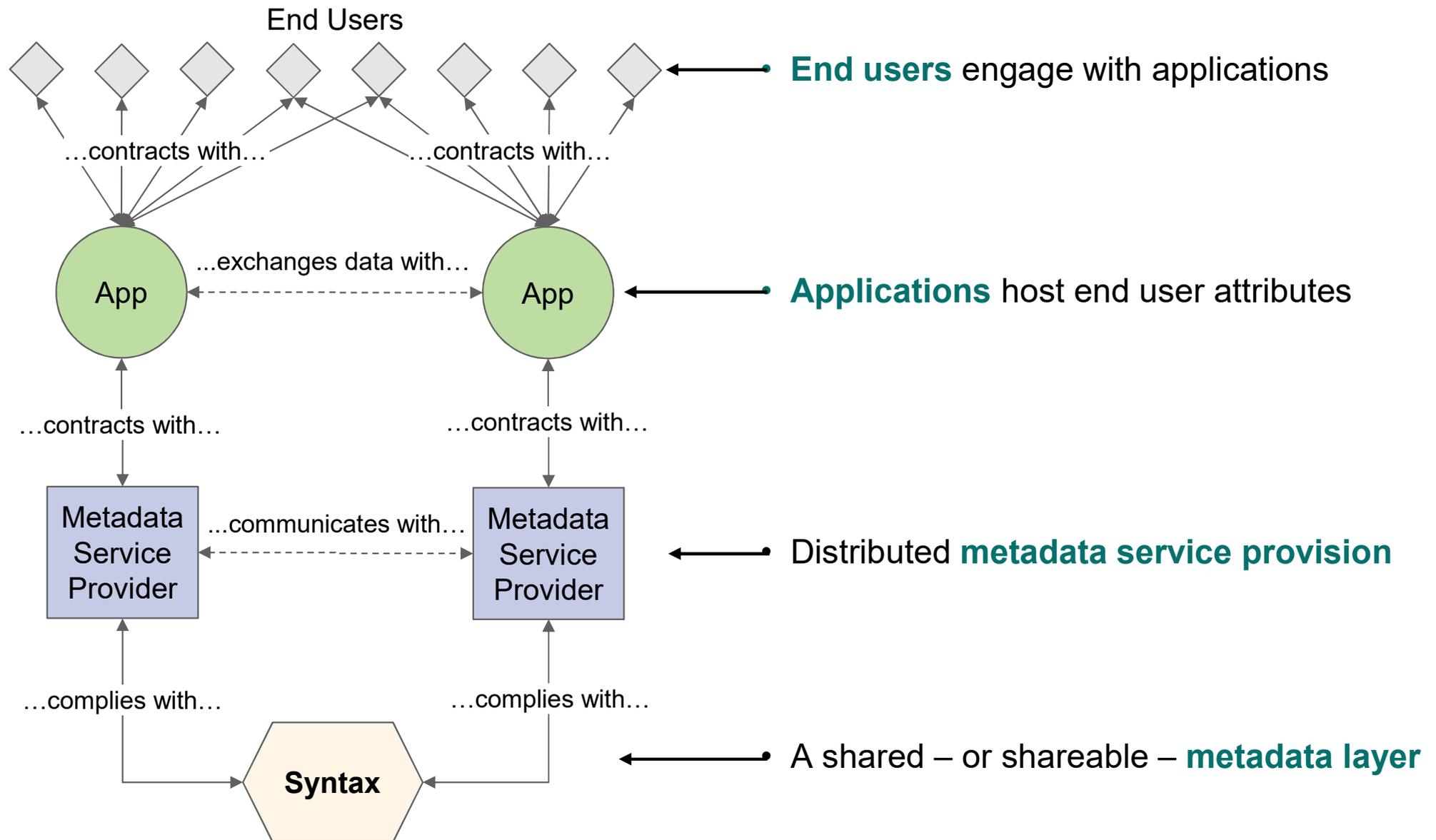
Verb	Definition
hasIssuedKnowledgeBasedChallenge	The Actor has issued a Knowledge Based challenge to verify a Claimant's relationship with evidence
hasPassedKnowledgeBasedChallenge	The Actor (e.g. claimant) has responded successfully to a Knowledge Based challenge
hasFailedKnowledgeBasedChallenge	The Actor (e.g. claimant) has responded unsuccessfully to a Knowledge Based challenge
hasSentActivationCode	The Actor has sent an activation code to the claimed identity (e.g. debit card]
hasRespondedActivationCode	The Actor (e.g. claimant) has responded successfully and used the activation code
checkedPhysiologyEvidence	The Actor checked that the Claimant's appearance was consistent with Evidence Attribute Profile (e.g. sex, age)
checkedFacePhotoInPerson	The Actor checked the face of the Claimant in person, to compare to photo image from evidence
checkedFacePhotoRemote	The Actor checked the face of the Claimant remotely (e.g. video link), to compare to photo image from evidence
checkedBiometricsPhysical	The Actor checked that Claimant's biometrics matched those contained in the Evidence, using physical tools
checkedBiometricsDigital	The Actor checked that Claimant's biometrics matched those contained in the Evidence, using digital technology

Illustration: overlapping semantic references



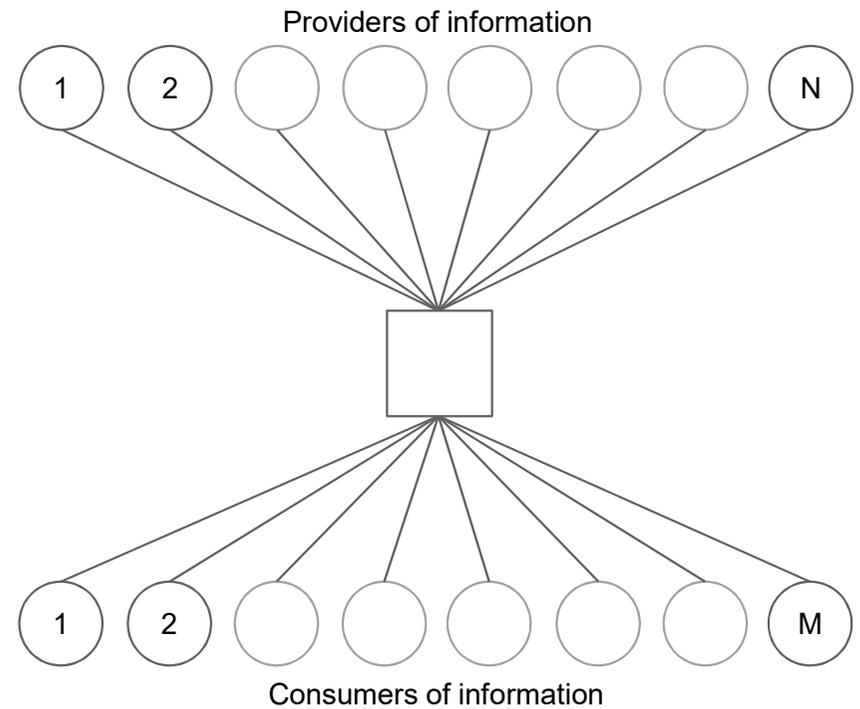
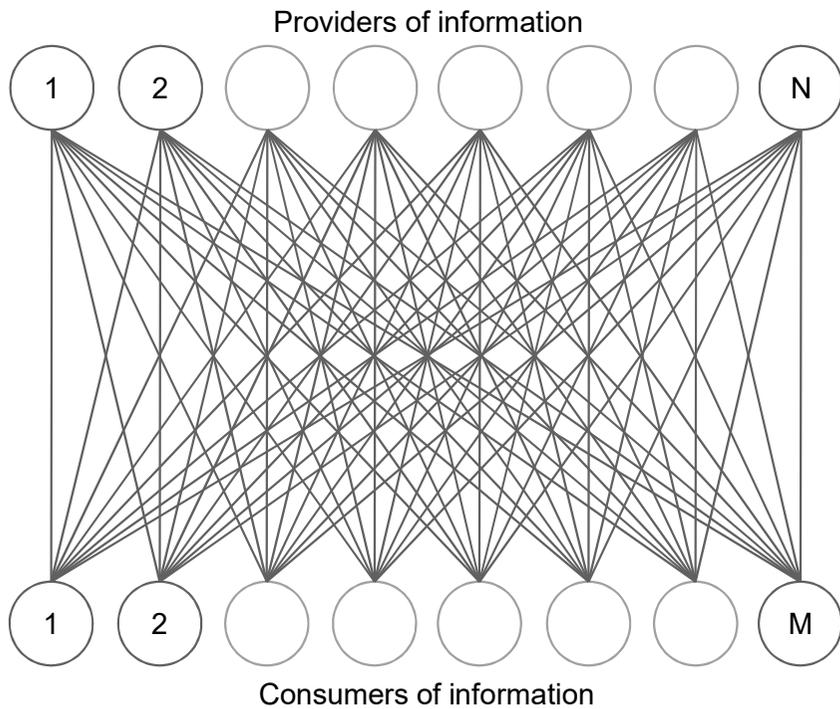
As an ecosystem, we....:

Store (and explicitly manage) Facts separately from attributes



As an ecosystem, we....:

Avoid the need to rely on a single technology / point of failure



As a Relying Party, I...:

Specify my requirements as a machine readable template

Description: Natural Language

Human Readable

Illustrative: JMLSG Guidelines

Description: Structured Language

Human and Machine Readable

Required data set

Execution: code

Machine Readable

Matching engines

Electronic ID&V

The standard level of confirmation, in circumstances that do not give rise to concern or uncertainty, is:

- *One match on an individual's full name and current address, **and***
- *A second match on an individual's full name and **either** her/his current address **or** his date of birth*

Name

Address

DoB

Required Assurance Level

```
{Name, DoB} ∈ isCorroborated{x|x ∈ AP}
{Name, Address} ∈ isCorroborated{x|x ∈ AP}
x = Author of corroborating statement
AP = {Experian, CreditSafe, Equifax}
```



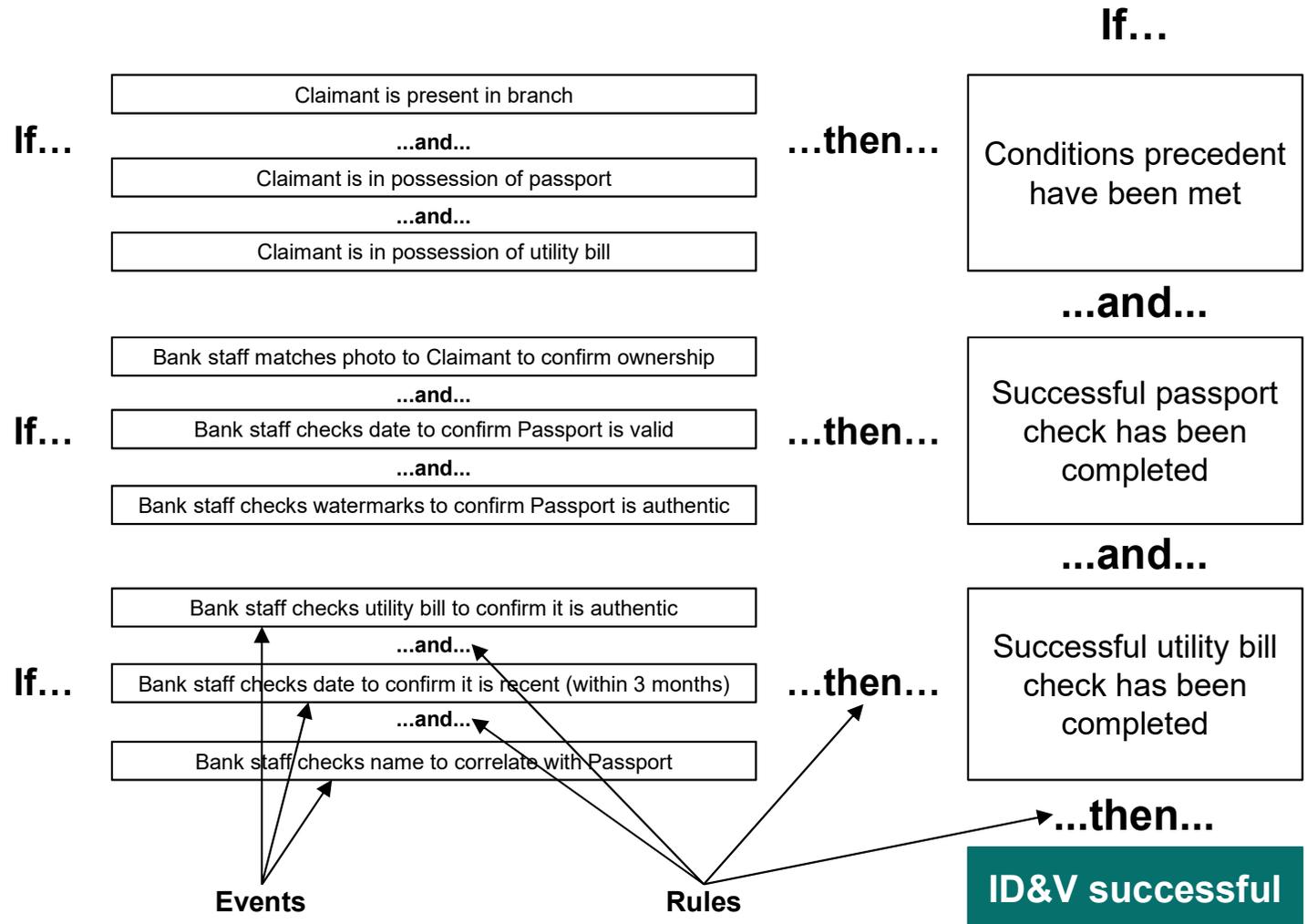
As a Relying Party, I....:

Use reasoning to combine Facts, assert *status* and place *trust*

Illustrative example: ID&V

JMLSG Guidelines for the standard Identification and Verification (ID&V) of a private individual:

- Identification: record full name, date of birth and residential address of the individual
- Verification: obtain documentary or electronic evidence from reliable sources, independent of the individual
- Standard workflow: verification against document with a photo (e.g. passport) **and** recent document with address (e.g. utility bill)



As a Service Provider, I...:

Develop different reasoning models, for use by Relying Parties

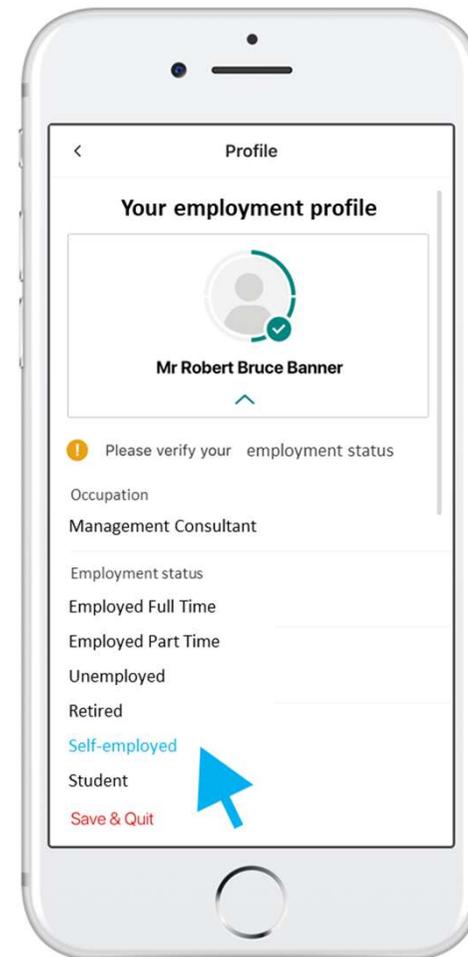
Authority	I know that Ben is Ben, <u>because</u> a trusted authority (e.g. an authorised identity provider) tells me that he is
Authorship	I know that Ben has a utility account with Eon, <u>because</u> Eon (i.e. the author of his account) has told me that Ben has an account
Consensus	I know that Ben owns this financial asset <u>because</u> Parties A, B, C and D all agree that he does
Correlation	I know that Ben lives at 30 Acacia Avenue <u>because</u> his wife is registered as living at 30 Acacia Avenue
Attestation	I know that this photo is a true likeness of Ben <u>because</u> two independent witnesses have signed and attested it to be as such
Usage	I know that Ben's mobile phone number is 07777 123456 <u>because</u> it has been used to respond successfully to several OTP checks
Inference	I know that Ben is over 16 years old <u>because</u> he has grey hair, a beard, bi-focal glasses, wrinkles and a stooped gait

As an Attribute Provider, I...:

Offer customers a valuable new service to manage their data

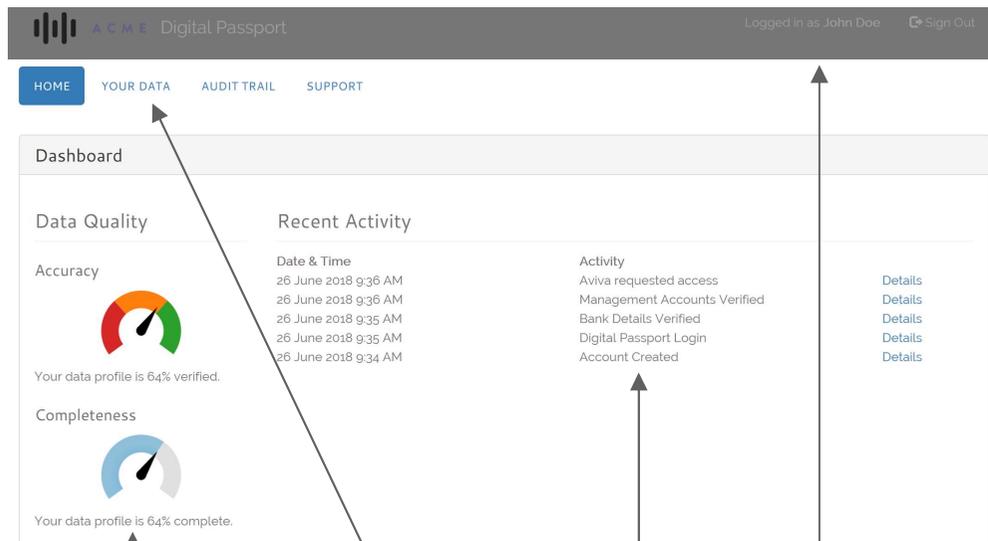
Example data management functionality

- Manage authorisations and consents
 - For use within an institution
 - For use externally
- Customer access to:
 - A history of communications
 - A history of activity
- Notification of:
 - Request for outstanding action
 - Confirmation of completed action
- View and manage Available Profile:
 - Add
 - Confirm
 - Amend
 - Delete
- View and manage evidence package:
 - Take photo / selfie
 - Upload document
 - Authorise access to data from another account



As an End User, I...:

Have the tools to manage Facts that relate to me and my profile

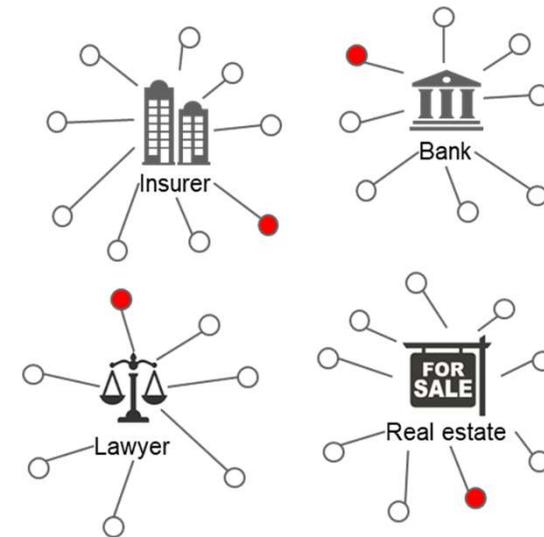


User control

Audit trail

Distributed data storage

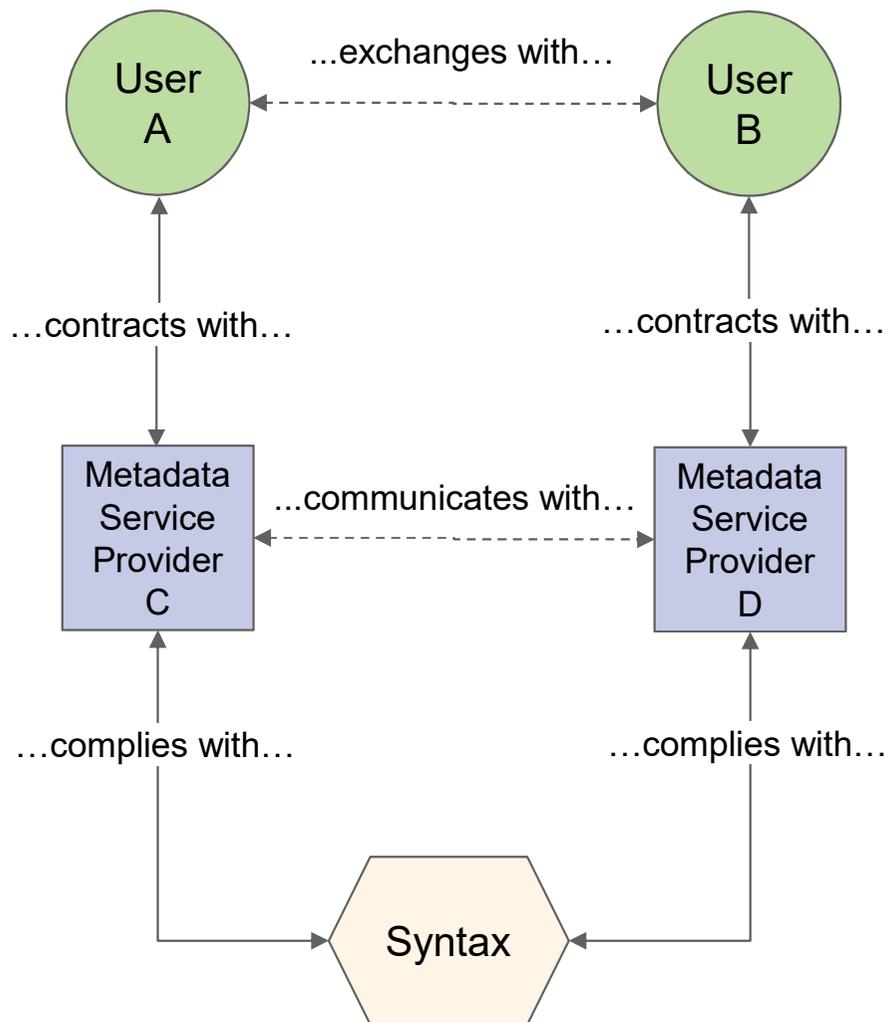
Trust scores (e.g. from Service Providers)



As a Metadata Service Provider, I...:

Earn a return on the work to store and manage access to Facts

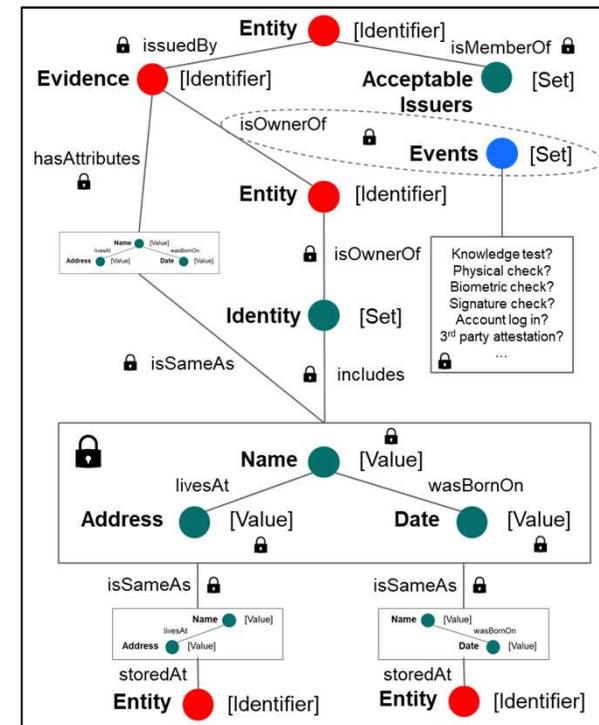
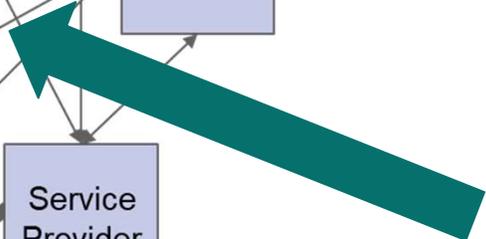
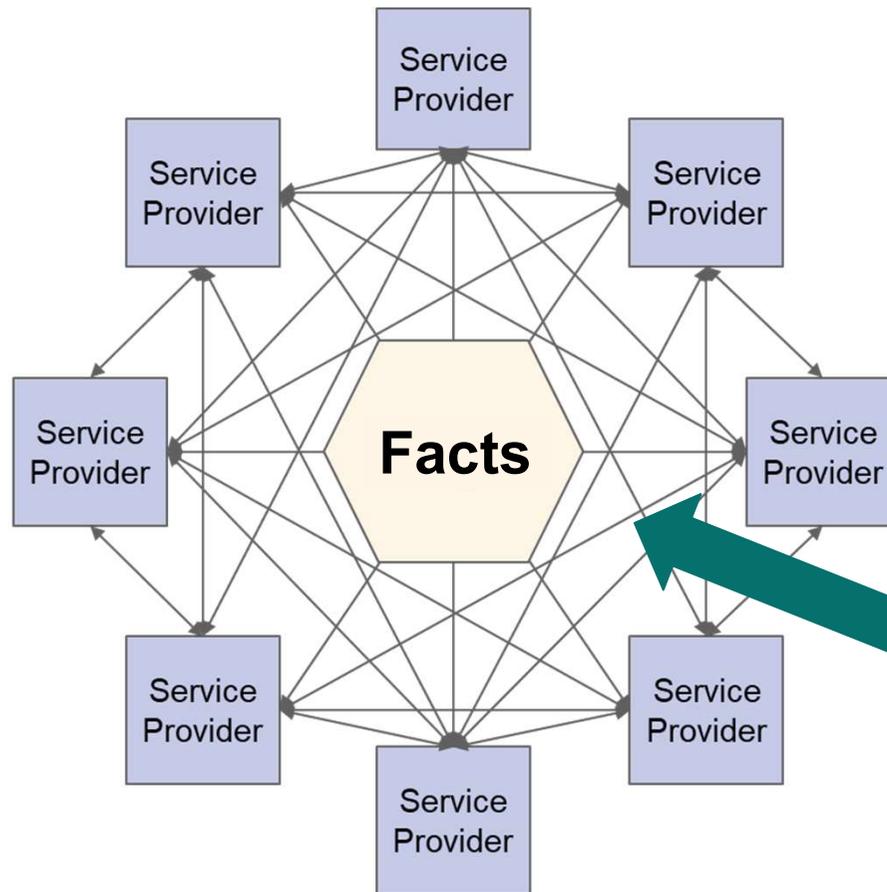
4-corner model



- **Directory:** allows users to publish the availability of data and services, and for other users to discover and consume them
- **Relationship mapping:** enables users to assert linkages between attributes and entities; map is amenable to graph theory
- **Event Log:** captures a complete and immutable audit trail of activity that is vital to compliance, assurance and governance
- **Permissioning:** manages authorisations at a field level; handles complex B2B situations; offers data owners a single point of control
- **Value-added services:** including e.g. template access requests, asynchronous routing, attestation / comments, watch / notification services, pricing of resources, etc.

As an ecosystem, we....:

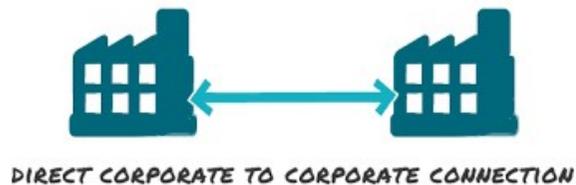
Create a consistent, meaningful and accessible metadata layer



| Supporting slides

Models of e-invoicing*

2 corner model



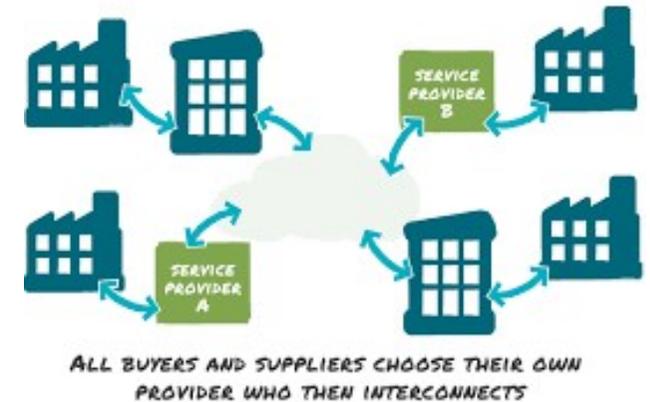
- Peer-to-peer process where the supplier and buyer directly **share documents** using EDI / XML files

3 corner model



- Supplier/buyer use the same third party service provider to **process e-documents** between them

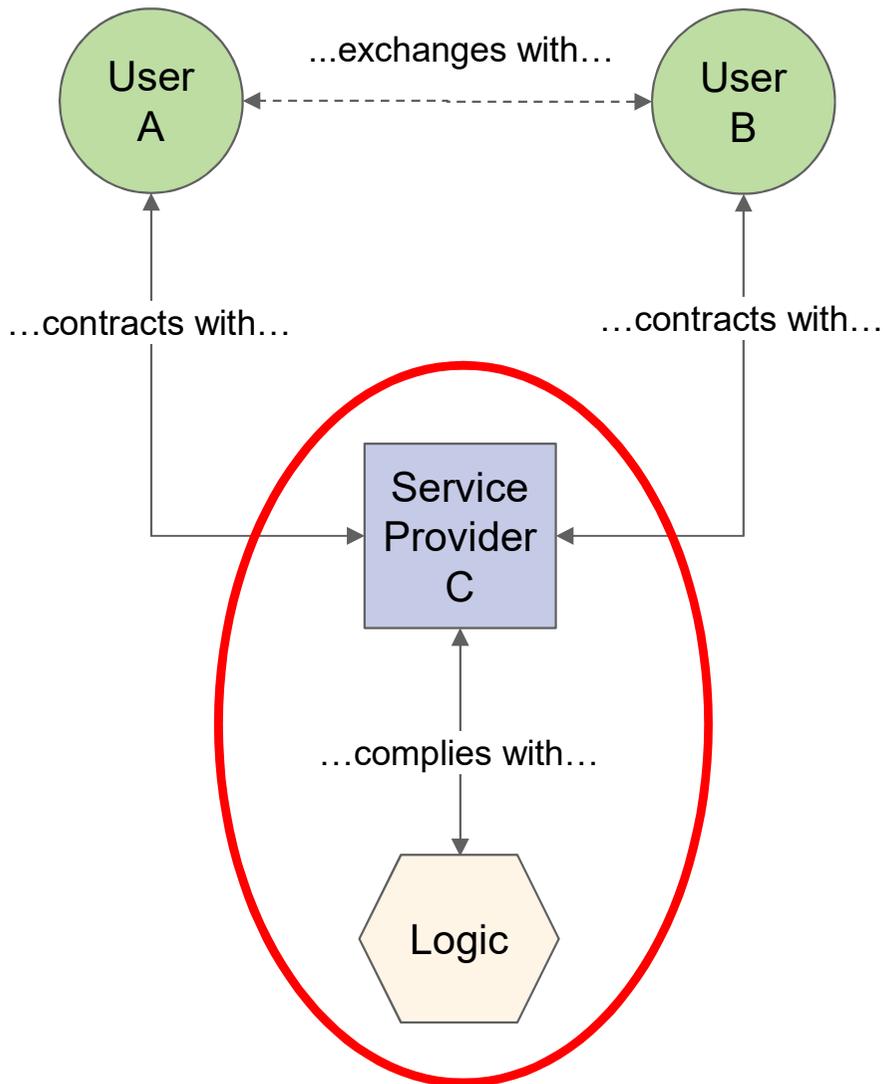
4 corner model



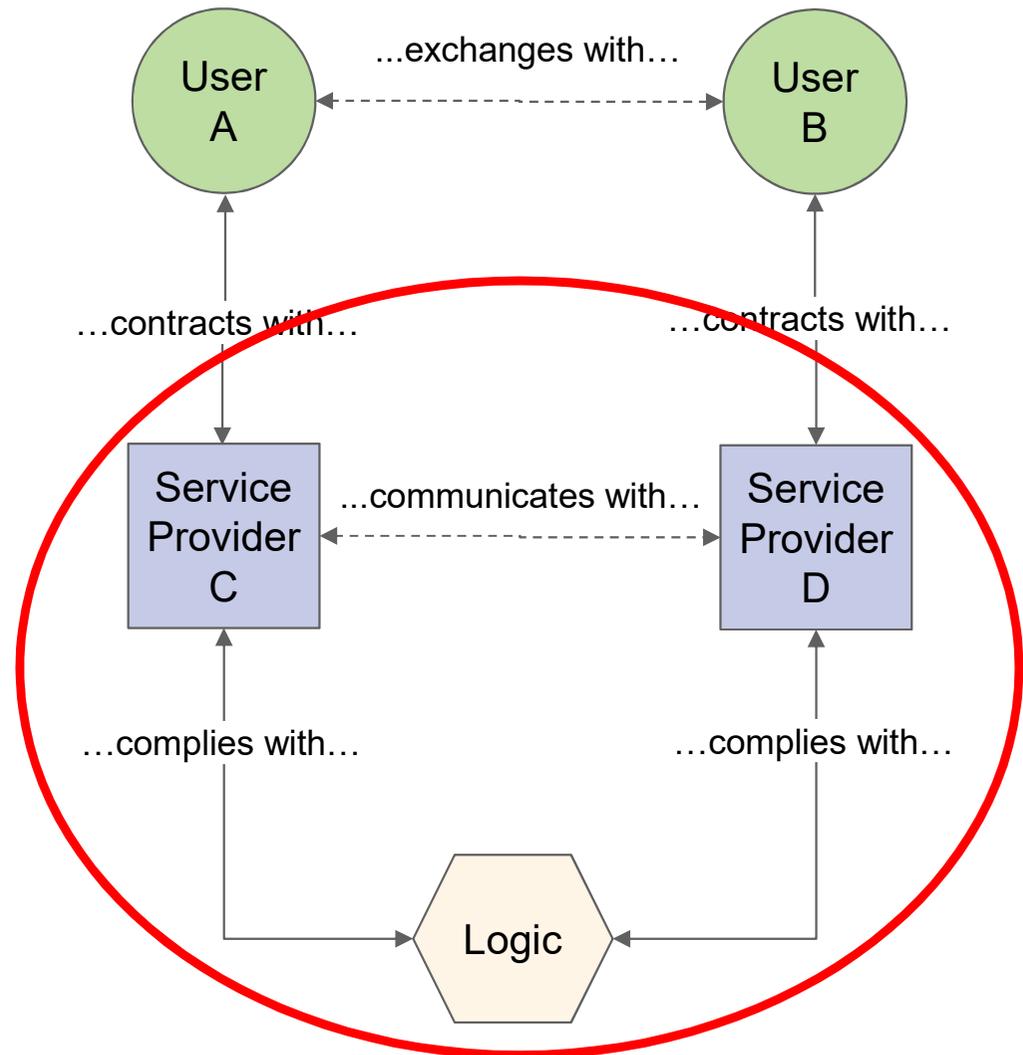
- Supplier/buyer use different service providers, who then collaborate with each other to **process e-documents**

Where is the work being done?

3-corner model



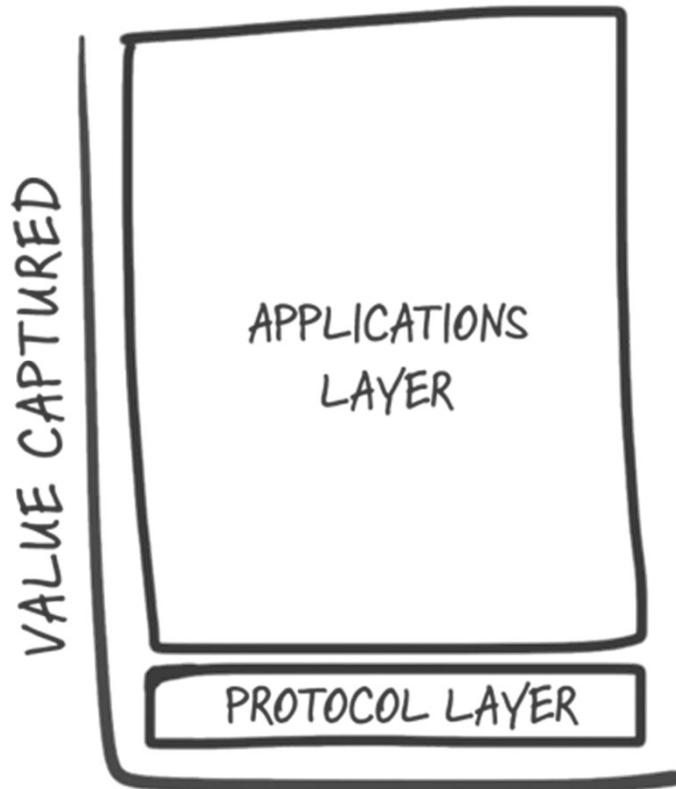
4-corner model



The advent of 'fat protocols'

3-corner model

The Web



4-corner model

Blockchain

