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?
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?

![Diagram showing the relationships between entities and attributes.](image-url)
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?

- **Trustable**
  - Can the attribute be corroborated?
  - Can the linkages be corroborated?
  - What due diligence has been done?
  - Who did it?
  - Does it meet my needs?
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

- Describable
  - Objects

- Relatable
  - Linkages

- Trustable
  - Events

- Accessible
  - Permissioning

- The Attribute Assurance Domain comprises of objects, linkages, events and permissions
- Express this domain as a set of statements: “Facts”
- A “Fact” is a statement that conforms to a core syntax
- All “Facts” are themselves addressable as objects
- The same mechanism can be used to access “Facts”, regardless of where or how they are stored
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

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

- UK Passport
- UK / EU Driver’s Licence
- EU National ID Card
- Student Union Card
- Employee Pass
- Rail Photocard
As an ecosystem, we...:
Share vocabularies to make more Facts relevant to each other

Example: events to check evidence belongs to a Claimant

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

Illustration: overlapping semantic references
As an ecosystem, we:

- Store (and explicitly manage) Facts separately from attributes

- End users engage with applications

- Applications host end user attributes

- Distributed metadata service provision

- A shared – or shareable – metadata layer
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

**Required Assurance Level**

\[
\begin{align*}
\{Name, DoB\} \in isCorroborated\{x | x \in AP\} \\
\{Name, Address\} \in isCorroborated\{x | x \in AP\} \\
x = Author \ of \ corroborating \ statement \\
AP = \{Experian, \ CreditSafe, \ Equifax\}
\end{align*}
\]
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)

\[ \text{If...} \]

- Claimant is present in branch
- Claimant is in possession of passport
- Claimant is in possession of utility bill

\[ \text{...and...} \]

- Bank staff matches photo to Claimant to confirm ownership
- Bank staff checks date to confirm Passport is valid
- Bank staff checks watermarks to confirm Passport is authentic

\[ \text{...and...} \]

- Bank staff checks utility bill to confirm it is authentic
- Bank staff checks date to confirm it is recent (within 3 months)
- Bank staff checks name to correlate with Passport

\[ \text{...then...} \]

- Conditions precedent have been met
- Successful passport check has been completed
- Successful utility bill check has been completed

\[ \text{...then...} \]

- ID&V successful
As a Service Provider, I...:
Develop different reasoning models, for use by Relying Parties

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

* Source: cloudtradenetwork.com
Where is the work being done?

3-corner model

User A ↔ User B

Service Provider C

...contracts with...

...exchanges with...

...complies with...

Logic

4-corner model

User A ↔ User B

Service Provider C ↔ Service Provider D

...contracts with...

...communicates with...

...complies with...

Logic
The advent of ‘fat protocols’

3-corner model

The Web

APPLICATIONS LAYER

PROTOCOL LAYER

VALUE CAPTURED

Blockchain

APPLICATION LAYER

PROTOCOL LAYER

VALUE CAPTURED

4-corner model