



FACTERN

BUILDING A TRUSTED ENVIRONMENT

EVENT-BASED DATA ASSURANCE

PRIVATE AND CONFIDENTIAL

This project was a discovery phase, executed over the summer

Date	Milestone	Agenda	Project participants
May 31 st	Workshop 1	Review proposed ecosystem definition and high level target functional architecture	<ul style="list-style-type: none">• DWP• Factern• HMRC
June 21 st	Workshop 2	Use case examples from private, public and third sectors; use case for visualisation	<ul style="list-style-type: none">• Idemia• Inidsol• Mydex
July 4 th	Workshop 3	Finalise landscape review	<ul style="list-style-type: none">• Santander
August 1 st	Workshop 4	Review potential viable economic models	<ul style="list-style-type: none">• tScheme
August 15 th	Workshop 5	Review use case visualisation	<ul style="list-style-type: none">• Zonafide

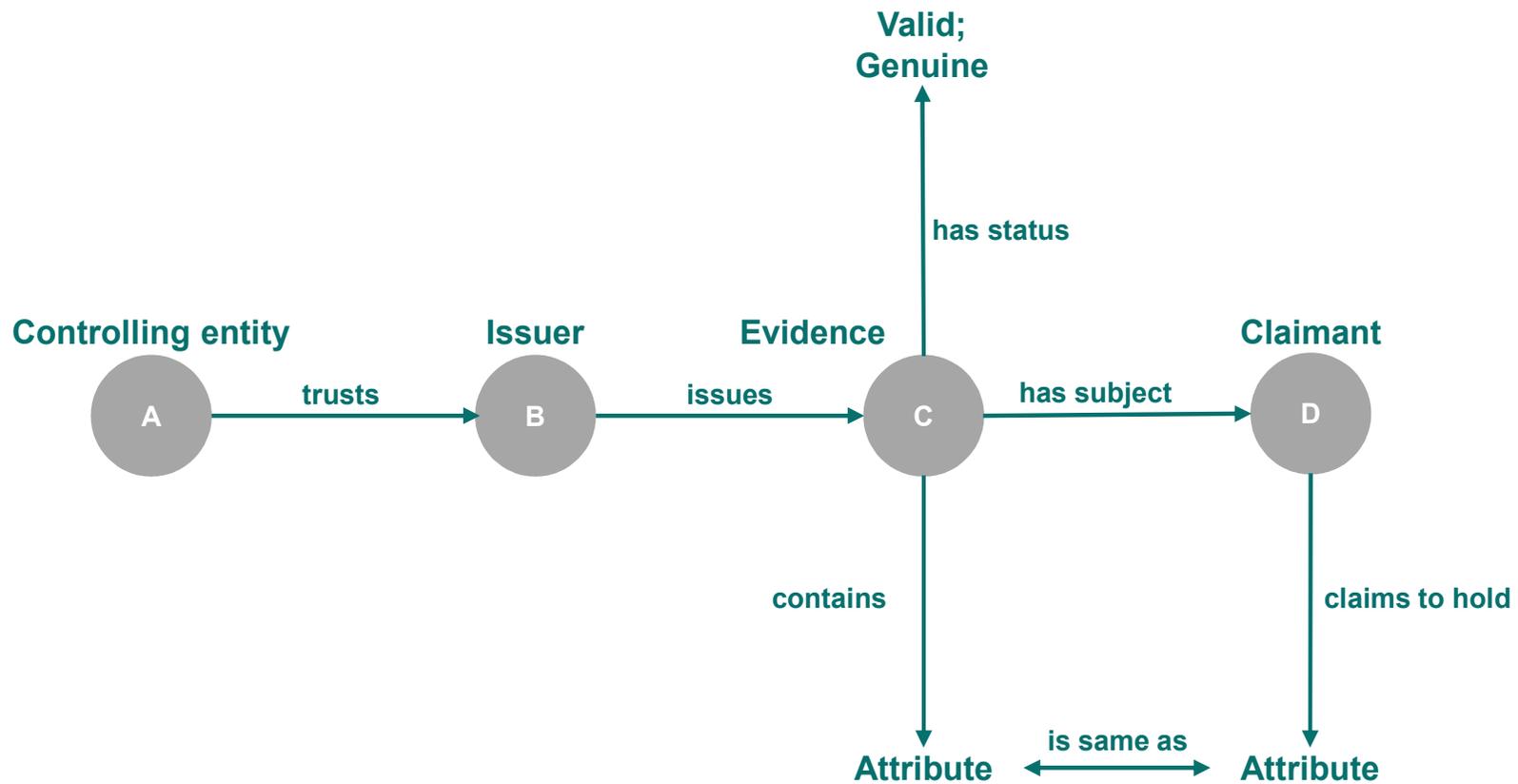
Hypothesis:

Events can be harnessed to improve data assurance outcomes

- Events can be used as inputs into models that use different forms of reasoning to validate and verify claims, providing a powerful and agile defence against fraud
- Relative to alternatives, Events are cheap to produce, publish, exchange and consume, and directly address the costs of duplicated effort
- Events capture the individual micro-transactions which are aggregated to form competing quality standards, enabling overlaps to be identified and re-used
- An Event-based approach federates trust to any entity with which we may have interacted, diversifying away from a reliance on a small number of sources
- Events offer a mechanism for 'thin file' citizens or customers to provide third party evidence to support their claims, even in the absence of traditional forms of proof

What do we mean by “Data Assurance”?

Investigating the nature of a claim

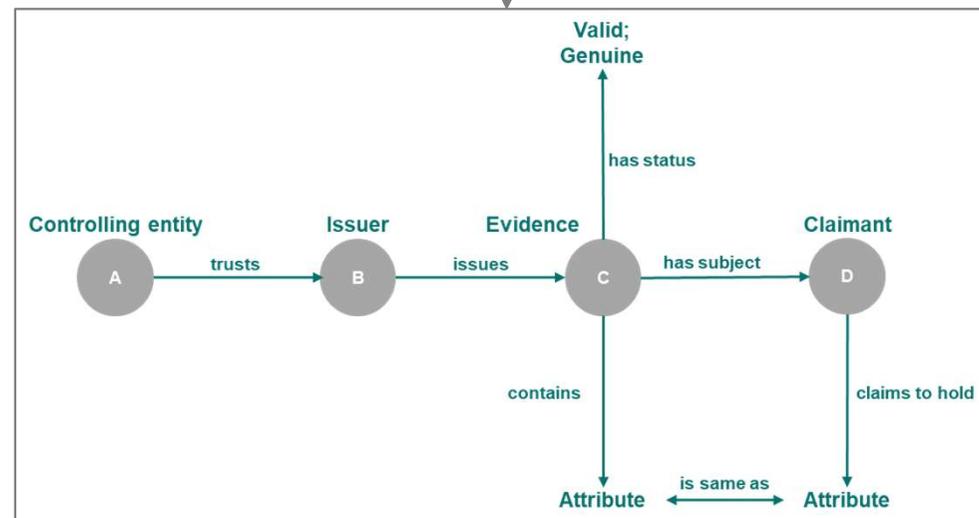


What do we mean by “Data Assurance”?

Assigning a status to a claim

“Controlling Entity A says that Claimant D holds [Attribute], to confidence level [X]”

Based on...



What do we mean by an “Event”?

- We define an “Event” as a trustable record of any attribute, relationship or activity that is made available as a digital resource for re-use by authorised third parties.
- **Trustable**:
 - An Event is a signed witness statement of the form: “X says that Y is true” ¹
- **Understandable**:
 - Events reference attributes, relationships or activities whose meaning has been defined – and can be shared – in a standard, relatable, machine-readable way ²
- **Accessible**:
 - An Event can be consumed directly (at scale) by automated reasoning engines
 - An Event is explicitly made available for re-use by authorised third parties
 - Access to an Event is governed separately to access to the data (i.e. attributes, relationships or activities) that the Event references

1. This is similar in form to a Verifiable Credential

2. Leveraging tools from the Semantic Web

What do we mean by an “Event”?

“Claimant A says that Claimant A is employed by Entity XYZ”

is not the same as:

“Witness B says that Claimant A is employed by Entity XYZ”

is not the same as:

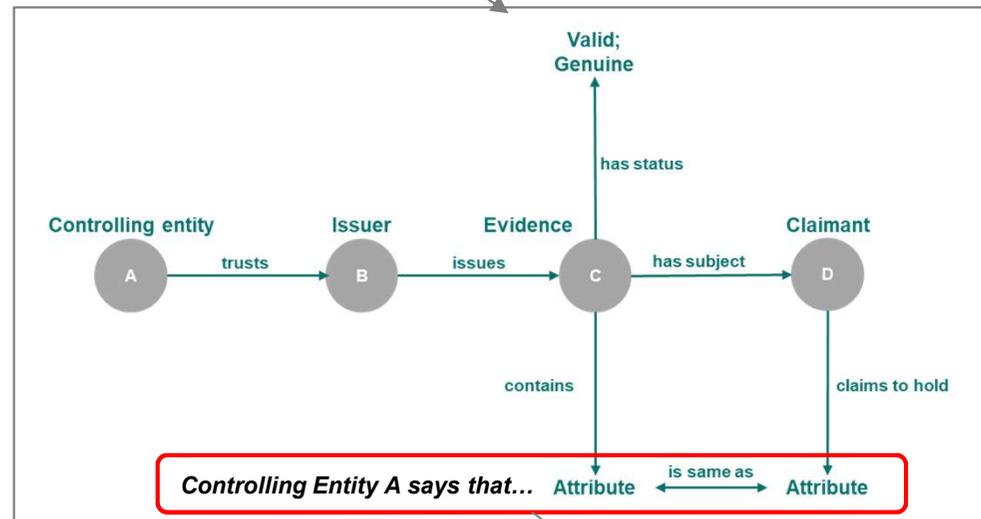
“Entity XYZ says that Claimant A is employed by Entity XYZ”

**3
separate
events**

What do we mean by an “Event”?

“Controlling Entity A says that Claimant D holds [Attribute]”

Based on...



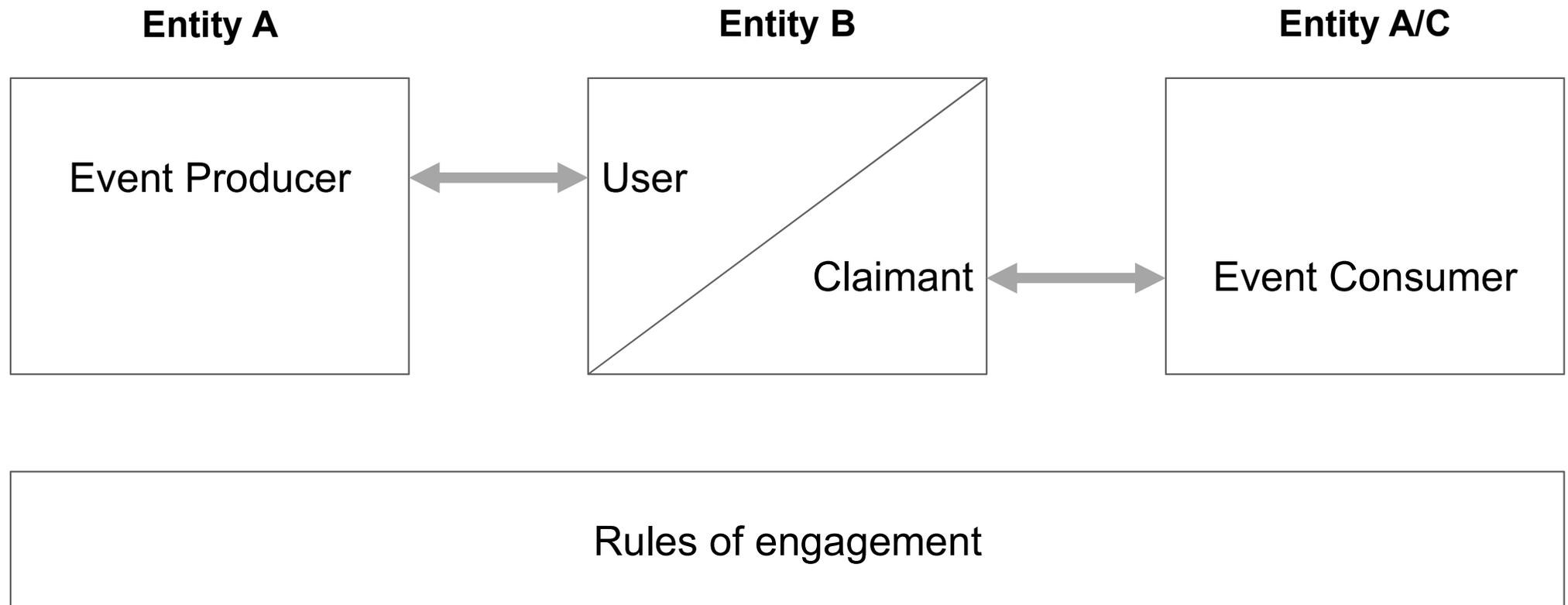
**3
separate
events**

Based on...

“Bob in the branch says that he had a quick look”

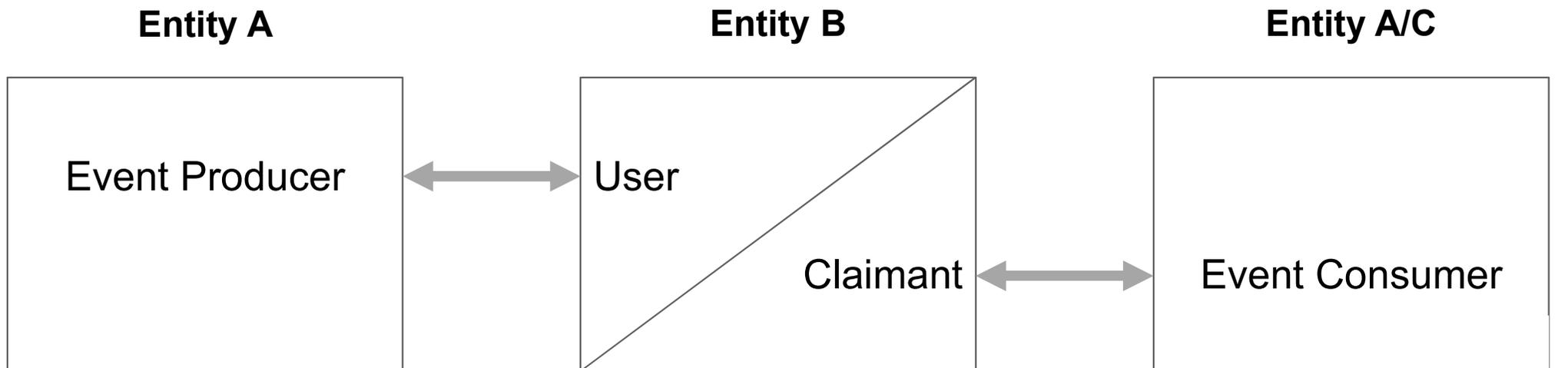
What do we mean by a “Trusted Environment”?

Relative roles within the ecosystem



Is there a viable economic model for the exchange of Events?

Motivation for each role



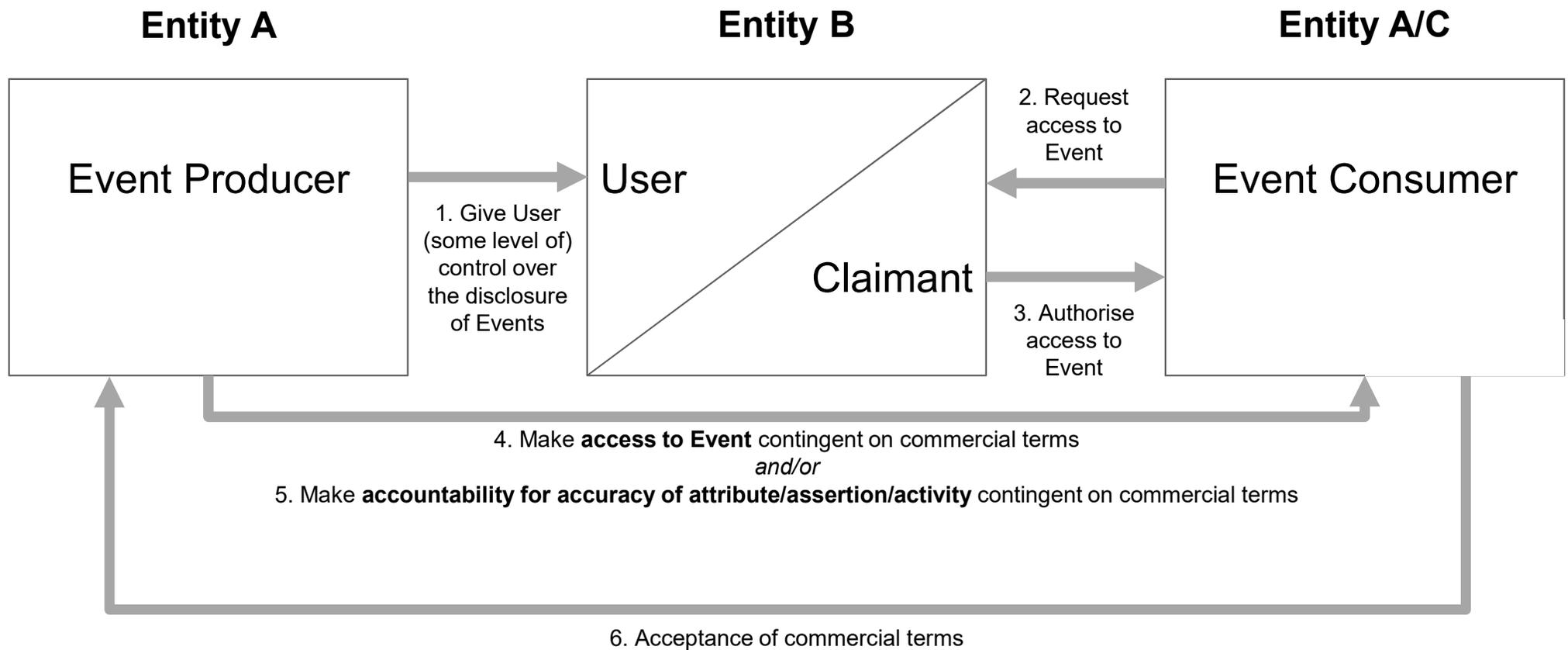
- Reduce cost
- Recover cost
- Broaden service offer

- Convenience
- Confidence
- Continuity

- Avoid cost
- Manage risk
- Improve experience

Is there a viable economic model for the exchange of Events?

Value exchange across the ecosystem



What infrastructure needs to be in place?

Rules of engagement

Vocabulary and semantics

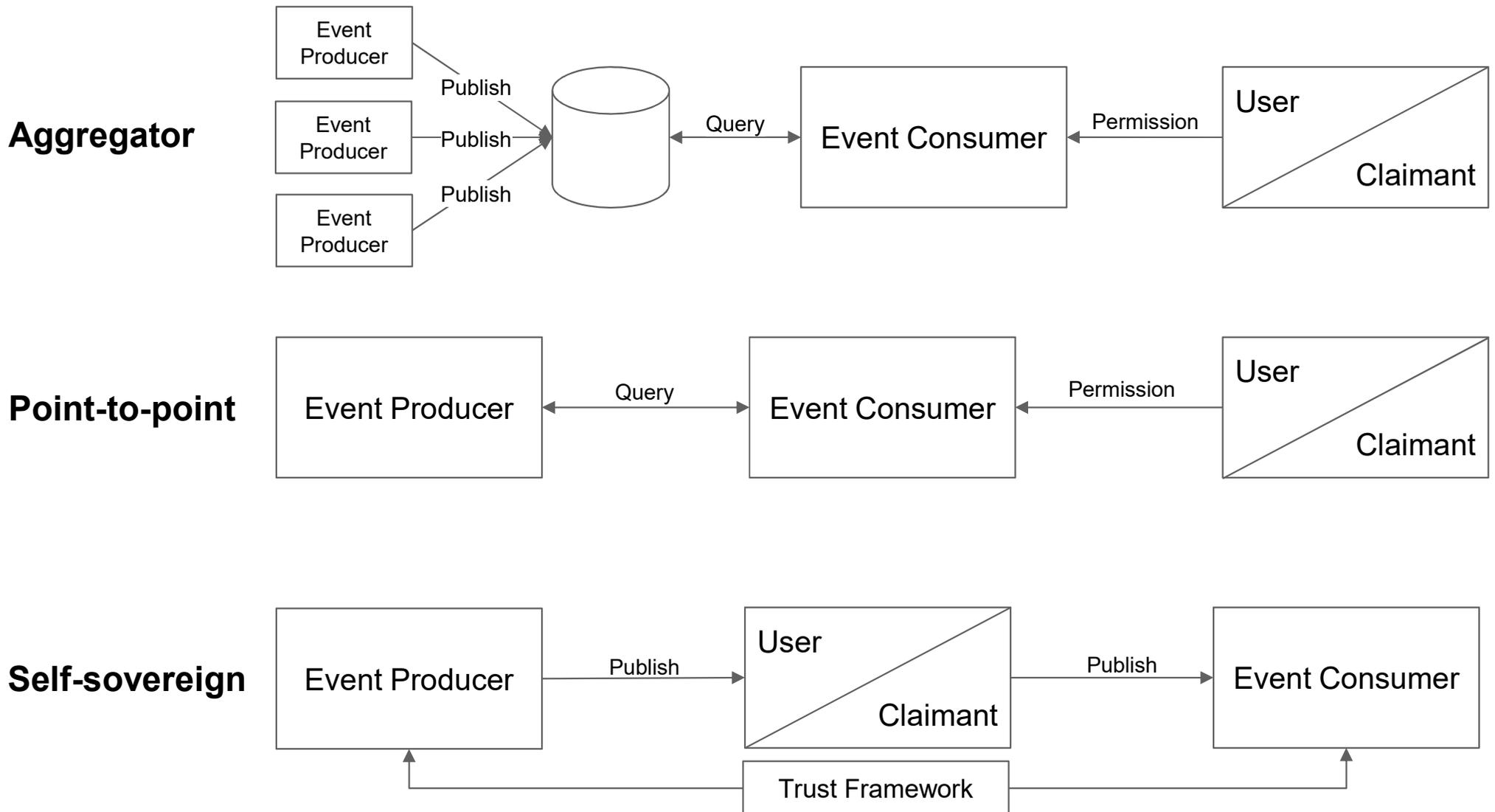
Discovery

Transport and trust

Contracting, accounting and settlement

What implementation options are there?

Example implementation options



Next steps

- Complete and publish Whitepaper
- Publish visualisation artefacts developed during course of the work:
 - Ontology: <https://ontologies.interition.info/webprotege/>
(https://youtu.be/pgLFLrx_av8)
 - Model queries and tests: <https://github.com/pjworrall/trustedenvironment>
 - Visualisation: <https://github.com/pjworrall/oixonsolid> (<https://youtu.be/ar-yof2Mkss>)
 - Model query endpoint: <https://fuseki.interition.info/>
 - Solid server used with the Visualisation App : <https://solid.interition.info:8443/>
- Establish and execute Alpha phase