Ecosystem Toolkit

Rules of Engagement

Building a Trusted Environment: Event-based Attribute Assurance

Alpha Project artefact

September 2020

FACTERN

OPEN IDENTITY EXCHANGE
White Paper

PROJECT PARTICIPANTS

The Open Identity Exchange (OIX) is a non-profit, technology agnostic, collaborative cross sector membership organisation with the purpose of accelerating the adoption of digital identity services based on open standards. OIX's broad membership and independent nature have seen it develop a significant body of digital identity research, and it is a significant influencer working towards the development of a digital identity market.

The following individuals and organisations participated in the OIX Alpha Project that formed the basis of this Report:

- Factern: Ben Helps, Robbie Fraser
- GDS: Chris Allgrove
- Food Standards Agency: Sid Kalita
- Future Borders: Ross McDonald, Stephen Cowx, Tom Robinson, Paul Evans, Jake Luscombe
- HMRC: Nick Davies, Wayne Robinson
- Idemia: David Rennie, Richard Thompson
- Inrupt: Paul Worrall
- Oxford Semantic Technologies: Peter Crocker
- University of Lincoln: Steve Brewer

OIX and the authors would like to thank all the Alpha Project team members for their considerable contribution to the work.

CONTENTS

1. INTRODUCTION

The Rules of Engagement (RoE) are designed to allow separate entities to agree and execute a repeatable, scalable and extensible model for collaboration to enable the sharing of information and expertise.

The RoE are one part of an Ecosystem Toolkit comprising of two parts:

- A **Technical Specification**[1] that is based on open standards and provides functionality to enable the *execution* of scalable and extensible collaboration
- This **Rules of Engagement** document which is a default collaboration framework that facilitates the *agreement* required for scalable, extensible and repeatable collaboration

This document both defines the RoE and sets out how Ecosystem Participants can use the Technical Specification to reference collaboration frameworks that go beyond the RoE.

In this way, each Ecosystem can combine the Technical Specification with their own collaboration framework.

[1] See separate document

2. RULES OF ENGAGEMENT

2.1 PRINCIPLES

Both the Technical Specification and RoE **must** be considered a minimum set of requirements. Entities that comply with this minimum set of requirements are referred to as Ecosystem Participants.

Pairs and/or groups of Ecosystem Participants **may** collaborate to share information in a given domain of interest by using the functionality defined in the Technical Specification and by adhering to the RoE.

Pairs and/or groups of Ecosystem Participants **may** also collaborate on a mutually agreed basis by opting to use a collaboration framework that goes beyond the RoE. Such pairings or groupings are referred to as Ecosystems.

Any Ecosystem Participant **may** initiate an Ecosystem. Potential Ecosystem Participants must be invited to join a given Ecosystem and may collaborate within the ecosystem once they additionally make a decision to opt in. These commitments are recorded as Events using implementations of the Technical Specification.

By definition, a given Ecosystem excludes all Participants which either choose not to opt in or are not invited to join. The rationale for exclusion can be opaque: they may be unable to meet the incremental requirements set out in the Ecosystem's collaboration framework, be unaware of its existence, be unwilling to join it or are simply not invited.

Whenever Ecosystem Participants share information, they **must** record the collaboration framework under which the transaction is occurring (although it is important to note that this record might not be something that is replayed with every transaction - for example, an Ecosystem Participant may specify that it is universally acting under a given collaboration framework for a given period of time):

- When information is being shared under the RoE, a set of minimum requirements is assumed to apply.
- When information is being shared under a collaboration framework that goes beyond the RoE, Ecosystem Participants must reference artefacts which collectively comprise the basis for collaboration within the Ecosystem.

Whenever Participants form an Ecosystem that references a collaboration framework that goes beyond the RoE, they **must** take responsibility for monitoring and enforcing compliance with that collaboration framework (e.g. through systems for issue identification, escalation, resolution, remediation, etc.).

It is **best practice** for 'open' Ecosystems (e.g. market places, extended supply chains) to make the reference to such artefacts public to all other Ecosystem Participants.

'Open' Ecosystems **must** configure such artefacts in terms of standardised models, component parts and easily accessible, repeatable patterns. These component parts must separate concerns and break granularity down to the level necessary to provision for 'policy as code'. Simply put, everything which can be separated out and configured/considered independently must be separated out and defined either as data or code in an implementation of the Technical Specification.

These **best practices** are designed to lower barriers to entry into a given Ecosystem. However, the Ecosystem Toolkit does not preclude or prejudice against 'closed' Ecosystems (e.g. collaborations based on statutory or regulatory requirements). There is no requirement to make the reference governance artefacts public to other Participants beyond those already party to the Ecosystem, or to use any particular form of governance.

2.2 DEFAULT CONFIGURATION OF PERMISSIONS / ENTITLEMENTS

The default configuration of the Technical Specification is to permit / entitle Ecosystem Participants to *write* Events, but not to *read* events. It is assumed that this default configuration complies with the vast majority of laws and regulations (i.e. everyone is

entitled to write down what they think, if those thoughts remain inaccessible to everyone) and would be considered to constitute security best practice.

Ecosystem Participants are responsible for ensuring that permissions / entitlements that extend beyond the default configuration continue to comply with all the national and international laws and regulations that are relevant to them.

In its fundamental structure, every Event includes a reference to the Rights Owner(s) on whose behalf the Event has been written. In many cases, the Ecosystem Participant will be the Rights Owner. In others, the Ecosystem Participant may be writing Events on behalf of another Rights Owner.

Ecosystem Participants can write their own Events, including Events that actively *grant permission* to themselves - or any other Ecosystem Participant - to read any other Event. Ecosystem Participants can also *remove permission* to read any given Event from any given Ecosystem Participant (including themselves) at any given time. Such permissions are also referred to as entitlements.

When writing Events on behalf of other Rights Owners, Ecosystem Participants cannot grant or remove permissions / entitlements over these Events. Ecosystem Participants are therefore responsible for:

- identifying Rights Owners
- providing Rights Owners with a service that allows them to configure permissions / entitlements over their Events
- authenticating Rights Owners

The legal and regulatory context in which each Ecosystem Participant operates will be specific to them and their domain of interest. Every Ecosystem Participant is responsible for the configuration of permissions / entitlements that comply with their specific legal and regulatory context.

The Technical Specification only provides a toolkit which enables permissions / entitlements for each individual Event to be configured in an easily *extensible* way, and to be executed in a highly scalable and machine-readable environment.

2.3 DEFAULT COLLABORATION FRAMEWORK

Whenever Ecosystem Participants share information under the Ecosystem RoE, a default collaboration framework **must** always apply:

- The default legal basis on which Ecosystem Participants share information is "consent" – i.e. the Ecosystem Participant is acting *on behalf of* the entities that act as Rights Owner(s) over the information being shared to configure permissions / entitlements according to their active instruction (as recorded by a further set of Events)
- The default liability limit under which other Ecosystem Participants access the Events being shared is zero – i.e. Ecosystem Participants rely on the information that they access at their own risk.
- The default assurance level of the events contributed by Ecosystem Participants is zero – i.e. the default expectation is that other Ecosystem Participants may choose the level of trustability they read into the information exchange, and may consider the information they are consuming on a spectrum of utility. Although the Technical Specification assures the *provenance* of Events, the RoE does not by default assure the *quality* of the information contained in Events.
- The default legal instrument under which Ecosystem Participants share information is the general body of national and international law and regulation that is relevant to each Ecosystem Participant. The RoE do not assume the existence of any other construct (such as a contract, memorandum of understanding, letter of intent, etc.) between the parties that might act as a further point of reference in the eyes of the legal or regulatory authorities.
- The default enforcement mechanisms are the general enforcement mechanisms provided by national and international legal and regulatory authorities (such as the courts, ombudsman, arbitration panels, channels for complaints, etc.). The RoE does not assume the existence of any incremental and mutually agreed systems for issue identification, escalation, resolution, remediation, etc.

- The default motivation for sharing information is altruism (i.e. acting for the greater good). The RoE does not assume any requirement for reciprocal value to be exchanged in return for the act of sharing information. As a result, the default value placed on the information being shared is zero, and therefore the RoE does not assume the need for any value settlement framework (beyond that of psychic reward).

Collectively and exhaustively, these components comprise the default collaboration framework that constitutes the RoE. This is the default artefact that is referenced by the Technical Specification.

3. ECOSYSTEM GOVERNANCE

By design, the RoE aims to set out a minimal basis under which information is exchanged. It is therefore desirable for Ecosystems to collaborate on the basis of collaboration frameworks that are tailored to their specific context.

When information is being shared under a collaboration framework that goes beyond the RoE, Ecosystem Participants **must** reference legal instrumentation which collectively establishes the legal basis under which the transaction is occurring (see Sections 3.1 and Section 3.2.1 below).

The RoE enforces a default legal basis of consent, but does not seek to define the legal basis appropriate for *any* given Ecosystem. Rather, its goal is help to associate the collaboration framework under which information is shared with the information itself, as a way of supporting the collaboration between the Ecosystem Participants that comprise the Ecosystem.

It is **best practice** for Ecosystems to use collaboration frameworks that are composed of artefacts which – over time – may become standardised points of reference for other Ecosystems. This facilitates the *agreement* required for repeatable, scalable and extensible collaboration, making it easier for Ecosystem Participants both to join existing Ecosystems and to initiate their own.

In this section, we consider two aspects of a given collaboration framework: firstly, we point to the spectrum of different legal instruments that might be used to define a collaboration framework; secondly, we highlight some of the different dimensions of collaboration that may be covered by such instrumentation and which collectively compose the collaboration framework itself.

We recognise that neither constitutes a comprehensive or definitive set, and can only act as an initial hypothesis for the “composability” of collaboration frameworks. The intention is for the Open Ecosystem Federation (OEF) to test this hypothesis in a Beta Project, by using the Technical Specification to reference a legally enforceable collaboration framework that

uses a collaboration agreement based on the default setting contained in the Rules of Engagement and extending across the components set out below.

3.1 LEGAL INSTRUMENTATION

There are a number of legal bases on which collaboration frameworks can be constructed. Taking the EU's General Data Protection Regulation (GDPR) as an example, there are six lawful bases for processing personal data: consent, contract, legal obligation, vital interests, public task and legitimate interests.

It is expected that the majority of Ecosystems that rely on a legal basis that goes beyond the default of consent set out in the RoE will do so under contract. The precise nature of the contract used to articulate a given collaboration model may vary. For example, it is easy to identify at least three such variants:

- Bilateral contract
- Multilateral collaboration agreement
- Bilateral contracts with a legal entity tasked with operating a scheme

Given the expected use of a contract in the form of a collaboration agreement to support the Beta phase, we use this section to focus on this particular variant of legal instrumentation. The Appendix elaborates further on contracts organised bilaterally or as a scheme.

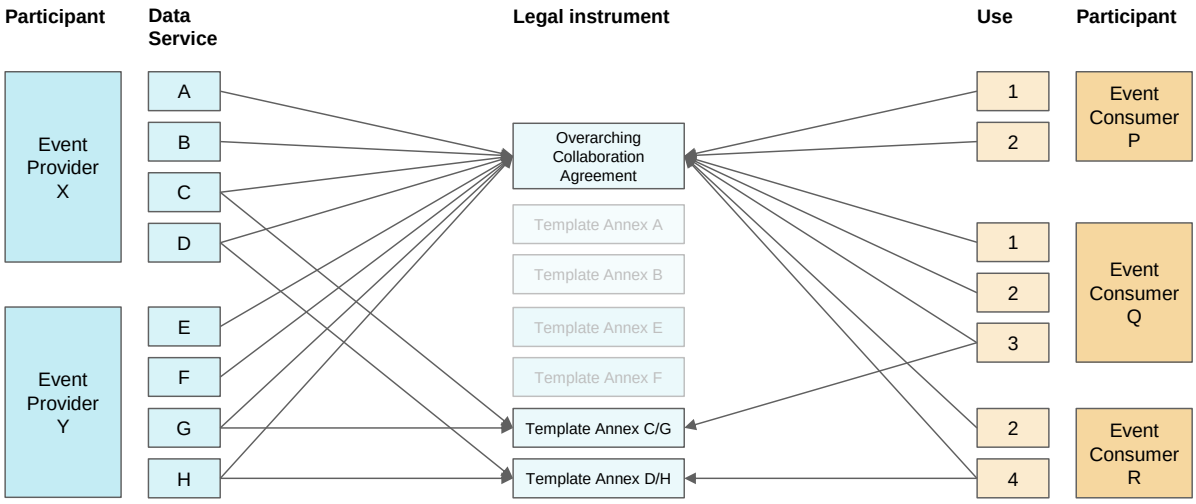
A collaboration agreement is a contract that covers multiple data services and uses, using template annexes to reflect any incremental dimension of governance that is specific to a particular data service and/or use.

The collaboration agreement governs the information exchange between *several* Ecosystem Participants acting as Event Producers/Providers, and *several* Ecosystem Participants acting as Event Consumers, all of whom choose to submit to the terms which it contains.

A collaboration agreement therefore provides a common artefact which can be referenced by all the Ecosystem Participants - in other words, unlike a master service agreement, it is a

multilateral agreement. The collaboration agreement may include the constitution of administrative roles and mechanisms to support the evolution of the agreement itself over time (see Section 3.2.7).

Figure 1: Collaboration Agreement



[Source: Pinsent Masons]

As the name suggests, collaboration agreements are likely to be best suited to ecosystems where the participants are actively looking to collaborate with one another to streamline the mechanisms through which agreement can be reached to share information.

It is **best practice** to reference an open and standard artefact as the legal basis for collaboration. For example:

- Where an Ecosystem Participant is making information available to all other Ecosystem Participants (e.g. as 'open data'), they may reference the terms of an open and standard licence.
- Where Ecosystem Participants share information multilaterally, they may invite others to participate under the terms of an open and standard collaboration agreement.

It is still possible for Event Providers[2] to compete to provide data services to Event Consumers under the terms of a collaboration agreement. However, they have agreed to do so under a common collaboration framework.

3.2 COMPONENTS

This section elaborates a non-exhaustive list of the different dimensions that Ecosystems might use to compose the collaboration framework under which they have mutually agreed to collaborate. These dimensions might be captured in a form of legal instrumentation (such as the examples in the section above), which in turn can then be referenced as the basis for information sharing via implementations of the Technical Specification.

3.2.1 Legal Basis

Ecosystems **may** share information on a legal basis that is different from the legal basis of "consent" that is the default under the RoE.

Taking the EU's General Data Protection Regulation (GDPR) as an example, there are six lawful bases for processing personal data: consent, contract, legal obligation, vital interests, public task and legitimate interests.

When personal data is involved, the GDPR imposes a high duty of care upon data controllers in selecting their data processing service providers. This duty of care may be reflected in specific clauses within the legal instrumentation.

[2] Note that we distinguish between an Event Producer (the Legal Entity responsible for *generating* an assertion) and an Event Provider (the Owning Entity responsible for the Expert System that refines the assertion into an Event and collaborates over it with other Expert Systems as part of an Ecosystem). In the context of the OIX Trust Framework, the Event Provider may be considered equivalent to the Broker role.

3.2.2 Liability Framework

Ecosystems **may** choose to accept a level of liability linked to the quality of the information being shared that is greater than the level of zero that is the default under the RoE.

A collaboration that includes a liability framework (linked to data quality standards and assurance levels) gives those Ecosystem Participants a basis for recourse if they rely on the information being shared.

3.2.3 Assurance Framework

Ecosystems **may** choose to specify a level of assurance over the quality of information on specific events that is greater than the level of zero that is the default under the RoE.

The Technical Specification enforces a level of assurance as to the *lineage* or *provenance* of information. However, it does not impose or generate any level of assurance about the *quality* of the information being shared – it may range from well formed but nonsensical to highly refined insight. Assurance framework specifics will depend on the context of the types of information exchange present in an ecosystem and the domains and subdomains over which the participants are intersecting.

3.2.4 Issue Resolution

Issue resolution mechanisms are closely linked to liability and assurance frameworks. These **may** involve mutually agreed procedures to identify, remediate and resolve issues, as well as sanctions for ecosystem members that fail to observe them (e.g. expulsion from the ecosystem).

3.2.5 Terms of Service

Ecosystem Participants **may** use an implementation of the Technical Specification to reference terms of service that cannot (yet) be expressed within the ontology. These might include service levels, feedback loops, revocation rights, etc.

For example, Ecosystems **may** choose to specify a service model that is designed to encourage members to behave as good ecosystem "citizens" and to minimise the need for escalation of issues by alerting Event Providers to issues with their data service on the basis that the Event Provider will use the feedback to address the issues - and improve data services - in a timely manner.

3.2.6 Scope of Service

The default scope of service within the Technical Specification is the provision of access to write information in the form of Events. The Technical Specification defines the service via its core administration responsibilities and ontology.

Ecosystem Participants **may** expand the administrative responsibilities and ontology to express key features of this service (such as time-to-live, access expiry, etc.) and to express an expansion of the scope of service (such as mirroring, notifications, etc.).

3.2.7 Ecosystem Intent

Ecosystem Participants **may** use an implementation of the Technical Specification to reference a mechanism that defines the intent of a given Ecosystem, beyond the immediate transaction involved in sharing information.

For example, intent may be used to capture what is expected of the members of the Ecosystem, what good reciprocation looks like, how common interests are protected, etc.

3.2.8 Membership Administration

An Ecosystem may use an implementation of the Technical Specification to reference artefacts used to administer its membership. Such artefacts might include (but are not limited to):

- The *people* or *entities* responsible for administration. For example, an Ecosystem operating under a collaboration agreement may appoint a 'Steward' to be responsible for maintaining the agreement and administering the process of members signing up to it
- The *policies* used to determine membership. For example, an Ecosystem comprises of members of a given club: to become a member of the club, parties must be recommended by at least one other member.
- The *mechanisms* or *tools* used to assign or revoke the attributes or characteristics required to participate in an Ecosystem. For example, the process for administering membership is handled using Github and Github accounts.

3.2.9 VALUE EXCHANGE FRAMEWORK

The default motivation for sharing information is altruism. The default value placed on the information being shared is therefore zero.

Ecosystem Participants **may** use an implementation of the Technical Specification to reference a value on the information being shared that is greater than the default value of zero that is the basis for the RoE.

Access to the information within that Ecosystem will then be contingent on settlement to that value. Best practice is to reference open and standard values (such as currency-based prices) to minimise barriers to entry.

3.2.10 SETTLEMENT FRAMEWORK

The default reward for those sharing information or expertise within ecosystems is “psychic reward” therefore unless configured otherwise via a Collaboration Agreement there is no value settlement framework in place.

Ecosystem Participants **may** use an implementation of the Technical Specification to reference a value settlement framework that is different to the default settlement framework that is the basis for the RoE.

Best practice is to reference open and standard settlement frameworks (such as currency-based payment schemes) to minimise barriers to entry.

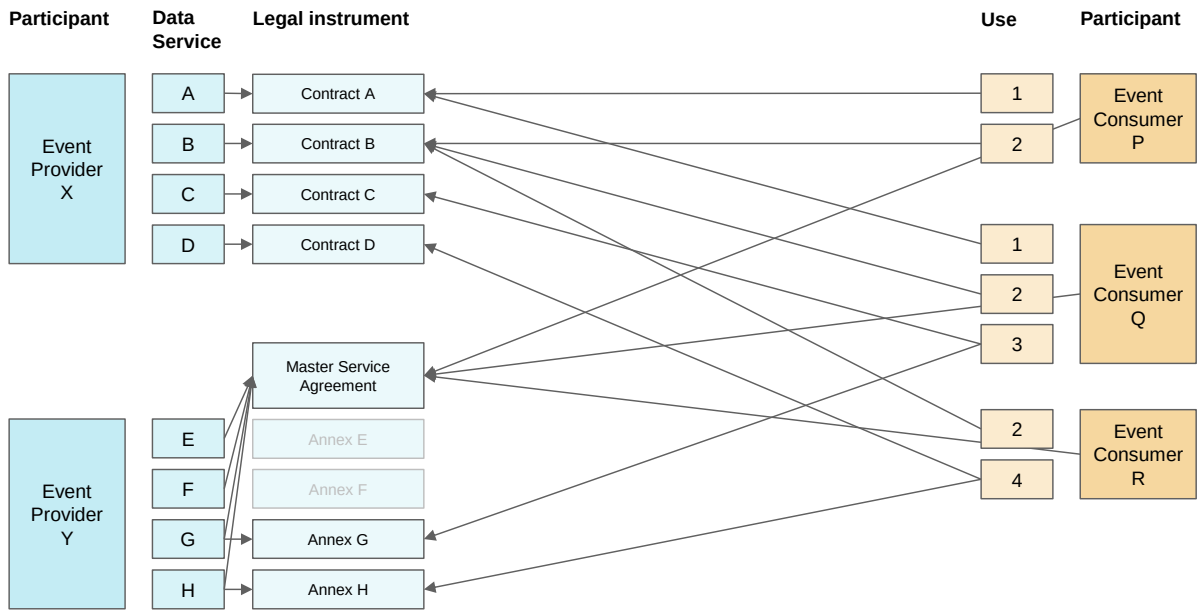
APPENDIX

BILATERAL CONTRACT

The second example of legal instrumentation is that of a bilateral contract between an Ecosystem Participant acting in the role of Event Provider and another Ecosystem Participant acting in the role of Event Consumer. The contract specifies the terms under which the Event Provider makes a given data service available to the Event Consumer for a given purpose or use.

The Ecosystem Participants use their respective implementations of the Technical Specification to reference the relevant contract as the primary artefact which describes the collaboration framework under which the information (in the form of Events) is being shared, as illustrated in Figure 1.

Figure 2: Bilateral Contracts between Event Providers and Event Consumers



[Source: Pinsent Masons]

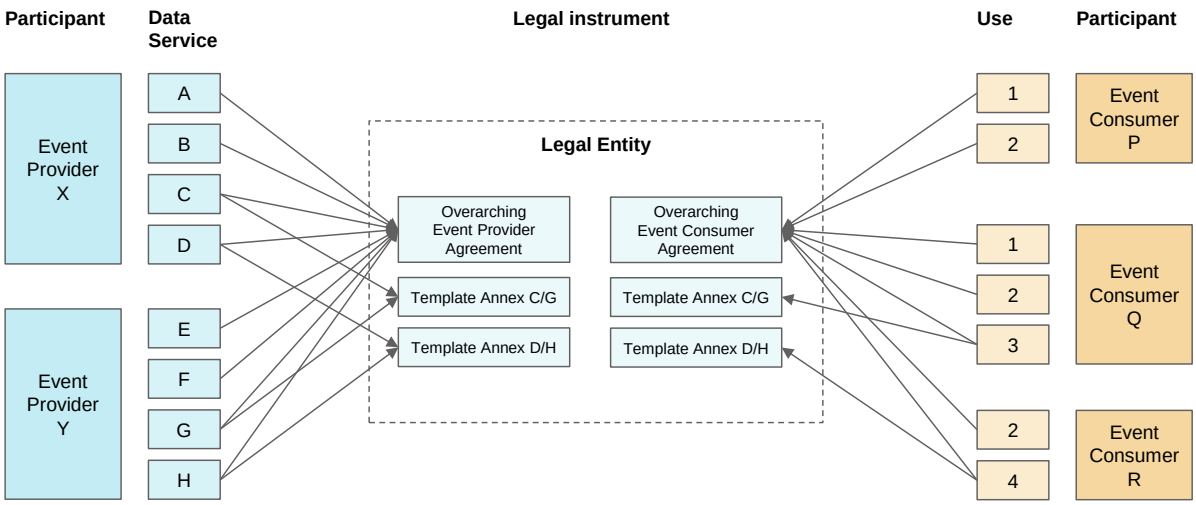
Contractual arrangements like this may be best suited to competitive ecosystems (e.g. markets) where different Event Providers compete to offer a range of data services. In such an environment, there may be competitive advantage in using a single contract that covers multiple data services and uses (e.g. a master service agreement).

SCHEME

The third example of legal instrumentation is that of a scheme. Each Ecosystem Participant that opts to join an Ecosystem governed by a scheme signs a bilateral contract with the legal entity that is tasked with operating that scheme.

Schemes are often used to mutualise the costs and risks inherent in sharing information. The existence of the legal entity dedicated to operating the scheme provides a vehicle for shared operations (such as dispute resolution and scheme administration) and shared risk management (such as access to balance sheet strength).

Figure 3: Scheme



[Source: Pinsent Masons]

Schemes provide the collaboration framework for many ecosystems already operating today, and the key properties of a scheme are desirable in many contexts. However, schemes can also have properties that make them undesirable in other contexts:

- Schemes can result in high barriers to entry into the ecosystem, leading to anti-competitive behaviour
- Schemes are usually very specialised in terms of the data services and uses in scope
- Schemes risk becoming 'gold-plated' and/or 'outdated' as the legal entity that operates is required to play an intermediary role but is constrained in its ability to innovate the way it executes that role

Although schemes provide an entirely valid collaboration framework for any Ecosystem, schemes that hold these properties work *against* the primary objectives of the RoE (i.e. to agree and execute a *scalable* and *extensible* model for collaboration through the sharing of information).