



## Position Paper

# Trust and Co-operation

### Problem

It is well-known that eCommerce transactions require a level of trust between participants in that trust, in this context, gives each partner confidence that the other will fulfil his part of a bargain in the future.

Trust, in this business context, relies primarily upon contracts (to specify the behaviour that is required) and an enforcement mechanism (to punish and deter non-performance). For this to work in an eCommerce environment, a process is required to register and verify each party's identity. However, the problem with registration processes is that they are hard to automate and, therefore, expensive. This creates a 'friction' that resists the growth of eCommerce.

The cost of registration can largely be reduced by sharing it between organisations. This is facilitated by mechanisms such as federation, which is designed to share identities and authorisations between organisations, thus extending their use. Today's federation mechanisms are oriented towards federating customer identity between members of a supply chain and, by agreement, between related supply chains. They aim to facilitate interactions between a customer and an organisation.

However, there is a need for federation between organisations; to make the federation process easier to automate; and to create new mechanisms, such as reputation, for sharing trust information.

Additionally, a common legal infrastructure, in the form of standardised contract templates, is required to facilitate de-perimeterized eCommerce.

### Why Should I Care?

- Trust is crucial to all human interactions and therefore the ability to express trust electronically is essential to successful electronic collaboration. (JFC#6)
- Registration and Trust Management, however, are expensive and often complex due to differing policy requirements
- De-perimeterization requires the ability to share reputation information between organizations (JFC#8)<sup>1</sup> and thus reduce costs.

---

<sup>1</sup> The term JFC#n refers to the relevant Jericho Forum Commandment number. See [www.jerichoforum.org](http://www.jerichoforum.org)

## Jericho Forum Recommendation/Response

The Jericho Forum believes that effective trust management is important in securing electronic transactions involving multiple organisations.

This paper sets out the Jericho Forum position on trust and concentrates on its use in the electronic business area. It sets forth a generic trust architecture framework within which trust decisions can be made and within which accountability can be supported. It then proposes the creation of a ‘trust broker’ to handle an organisation’s trust relationships.

### Background & Rationale

Within the context of this paper, trust can be either:

- A verb - A decision to rely upon someone’s future performance of a contract; or
- A noun - confidence that someone will meet a contract, based on their perceived capability, intentions and an accountability mechanism.

Whichever definition is adopted, trust is a vital pre-condition for successful collaboration<sup>2</sup>.

Central to this definition of trust is the idea of a contract. A contract involves two parties (which can be people or organisations), a set of rules about what each should do, and an accountability mechanism for handling failure by a party. A contract does not have to be a legal contract, written down and signed; it can simply be an informal code of behaviour within a community.

An accountability mechanism can include measures such as criminal prosecution, civil action, disciplinary action or merely ostracism from a community. Clearly, an accountability mechanism cannot function unless the identity of the failing party is known.

### Co-operation

Trust is an essential precondition for co-operation among people and organisations. It allows two parts of a transaction to be separated in time; for instance, a customer pays a supplier, expecting delivery of a product in a week’s time, because of trust in the supplier’s stated terms. A party chooses to co-operate with another in a trusting way because he believes some combination of the following:

- The trusted party is well disposed towards him
- It is in the trusted party’s best interests to comply
- The trusted party has the necessary competence, skills and resources to comply
- An accountability mechanism exists that can force the trusted party to comply

Trust is a social phenomenon; a wide variety of social structures have evolved over many years to encourage and enforce co-operation, ranging from marriage to contract law. Many of these were based in the past on face-to-face contact. Today, business and social interactions are increasingly being performed electronically. This creates new processes, such as authentication and authorisation, for managing trust. Authentication links an electronic agent to a real-world identity that forms the basis for an accountability mechanism; and authorisation represents a degree of trust or competency that has been assigned to the identity. An authorisation represents a contract, an agreed set of rules about how the holder and granter of the authorisation will behave.

### Organisations

People naturally create organisations, and an organisation has many of the legal rights of a flesh and blood person. For instance it is a legal person and can enter into contracts, but an organisation cannot *do* anything real. It must delegate its capabilities, either to owned equipment (plant), to people (employees) or to other organisations (sub-contractors) to fulfil contracts. Even contract signing must be delegated to employees and directors.

When organisations co-operate as potential provider and consumer of a service, the service provider has to ask the questions ‘*Am I prepared to work with this business?*’, and ‘*is this user empowered to commit his business to work with me?*’. The service consumer will enable its users by provisioning

---

<sup>2</sup> Note: trust is a risk management mechanism and should, ultimately, be considered within an overall risk management framework. For reasons of simplicity, we will not attempt to do that here.

them with authorisations on the service. It asks the questions ‘*Am I prepared to sign this service contract?*’, and ‘*Am I willing to allow this user to commit me to it?*’ before doing so.

In order to work together, organisations need to accept, and therefore understand, each others’ contracts. Increasingly this will need to be done in an automated way. Businesses also need to be able to account for the contracts/authorisations they have agreed to (both as producers and consumers) in order to understand the obligations they are currently under.

## Reputation

How does one party decide to trust another? It must decide whether the party is trustworthy or not, based on the proposed contract and a perception of the other party’s past performance. Good performance in similar areas makes it probable that the other party will be trusted. A record of performance constitutes ‘reputation’ – good or bad.

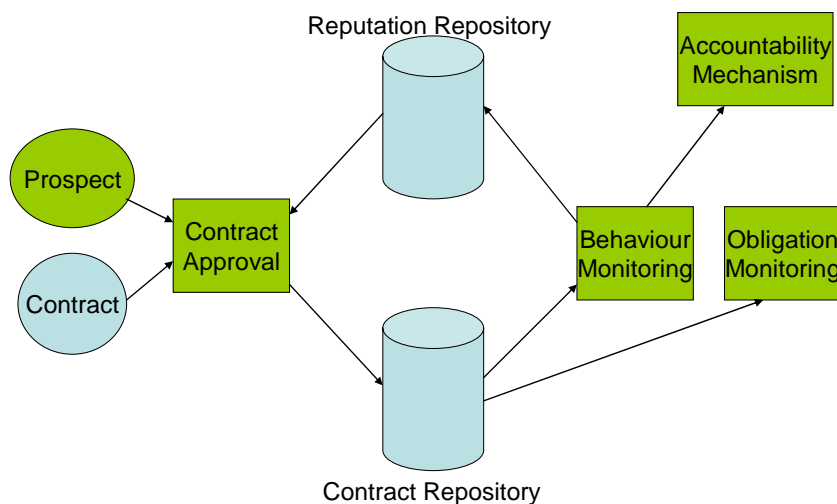
This begs the question of how two strangers can ever come to trust each other. Two mechanisms are possible here:

- parties may share reputation information with others they trust, allowing one party to take advantage of another’s experience; or
- a party may choose to trust a stranger in a small way initially, based on global accountability mechanisms such as the law, then escalate trust based on good performance

## A Trust Architecture

The figure below illustrates a potential trust architecture to implement these concepts.

Within the figure:



- The *Contract* is an agreement an organisation is considering entering into. This could be a business contract, or the allocation of a group membership in a directory
- The *Prospect* is the other party in the contract. This could be a user applying for membership of a group
- *Contract Approval* is the decision making process for whether or not to enter into the contract. It will use information in the reputation repository in making this decision
- If the contract is signed, it will be entered into the *Contract Repository* so the organisation can monitor its assets and liabilities. The contract repository can be considered to be part of the organisation’s accounts. In many organisations, the contract repository is implemented as group memberships in an LDAP user directory
- As the contract is executed by both parties, a *Behaviour Monitoring* process ensures that the trusted party is complying with the contract; and *Obligation Monitoring* ensures that the organisation itself is complying. In the electronic world, this is implemented by access management, provisioning and user audit
- The *Accountability Mechanism* is invoked if the other party is not complying with the contract

- The *Reputation Repository* records information that is known about other parties, their attributes and their past behaviour. This is the basis of contract approval decisions. It may be implemented by user attributes in an LDAP repository

Note: the examples given above relate to group memberships. Similar analogies could be applied e.g. license management or a shopping cart on a web site.

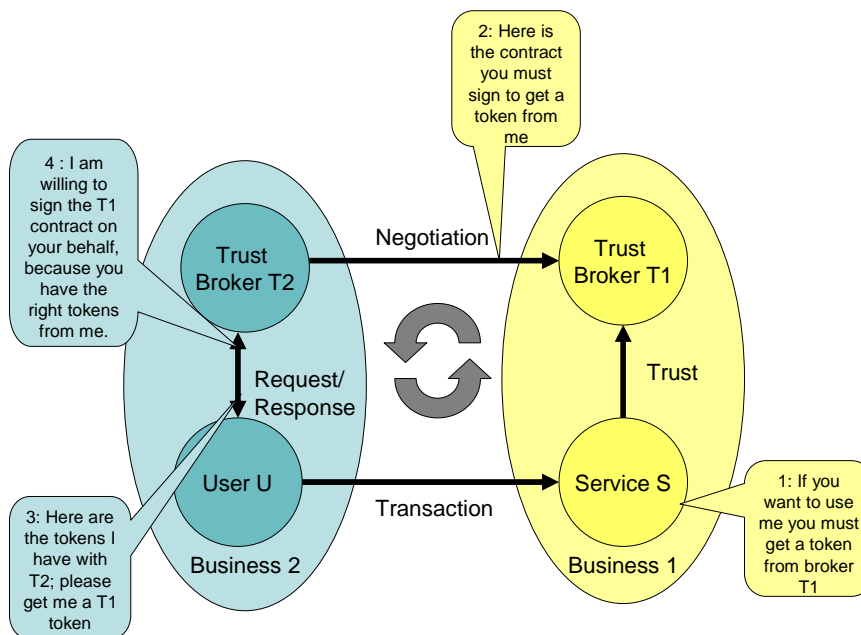
## De-perimeterization

The architecture above involves a single person or organisation acting alone. The Jericho Forum believes that the model should be generalised to support de-perimeterization.

One form of de-perimeterization comes from sharing reputation information between organisations. This can be done in several ways:

- Direct mechanisms such as federation
- Introduction protocols whereby one party can recommend someone to a third
- Market-oriented reputation services (of which modern day services such as Experian can be considered a fore-runner)
- Peer-to-peer mechanisms such as the eBay reputation system

The other form comes from improved mechanisms for delegating contracts. The Jericho Forum believes that existing access management and provisioning systems will evolve to being 'trust brokers'. The figure below illustrates a 'trust broker' concept.



The two businesses use trust brokers to control delegation of contracts between them. Initially this process would be mostly manual, but it will become more and more automated as authorisations become more standardised.

## Key Challenges and Next Steps

A variety of trust models are possible, with varying levels of technical implementation. The Jericho Forum should co-operate with The Open Group Security Forum to create a catalogue of such models. Of particular interest here is the rights smart contract model and the inherently secure E programming language proposed by Miller, Szabo et al. The Jericho Forum should also investigate the issues involved in standardising authorisations between organisations.

Vendors should develop trust broker (software and services) to link identities and authorisations between organisations.

Organisations should investigate the benefit to be gained from linking the agreement of a contract with provisioning it automatically. They should also consider the adoption of standard legal infrastructure to support de-perimeterization.