



# Trust Management - A Brief Overview

## Problem

Trust<sup>1</sup>, or the placing of it, is one of the key activities at the core of our human endeavours. The process of placing trust is simpler when the process is physical and proximal - that is when you can see, feel and touch that which you are about to trust. We have as human beings developed a number of risk management skills that we often cannot explain in concrete or scientific terms; “They looked shifty”, or “The bridge looked rickity”. These skills help us to decide whether or not to place trust.

The emergence of electronic networks that distance us from that which we want to trust introduce a number of new difficulties.

Simply put, we have not developed the appropriate mechanisms to place trust virtually, the requirements for which are clearly stated in the two *Jericho Forum Commandments*<sup>2</sup> JF#6 and JF#7 which come under the heading: **The need for trust.**

## Why should I care

As many will observe, this has been a problem for human beings since the invention of the carrier pigeon, and likely before. The growing criticality of the issue stems from the emergence and evolution of the Web, for such is the power of the Web that more and more of our daily activities are resulting in the need to place virtual trust, whether between two individuals, two enterprises, or between individuals and enterprises. At the same time there are forces at work whose aim is to suborn either the party we want to trust, or worse still the mechanisms or components we choose to use to connect to the remote party. There may even be occasions, in the virtual frame, where we are not even connecting to the party to whom we think we are connected.

All this has the potential to lead to one unfortunate outcome, and one that all markets fear; “Loss of Confidence”. One doomsday scenario is that the “Loss of Confidence” created by the current world banking crisis will be nothing when compared to the implications of the total breakdown in Virtual Trust that the Web might create. What would happen if no-one trusts the Web anymore?

On a more positive note, the ability to automate and improve the Virtual Trust processes between the relevant parties will provide the opportunity to make very large time saving process and procedural changes. Currently we mitigate the risks of Virtual Trust in a number of ways that costs time and money. If Virtual Trust could be achieved and maintained more

---

<sup>1</sup> Trust: is defined as assured reliance on the character, ability, strength, or truth of someone or something

Source: Merriam Webster Online Dictionary

<sup>2</sup> Jericho Forum Commandments (design principles) – available from [www.jerichoforum.org/publications](http://www.jerichoforum.org/publications)

easily the potential for value generation should not be underestimated. Imagine a world where short term contracts can be created in seconds, and terminated just as quickly.

## Recommendation/response

There are a number of capabilities that we need to develop or strengthen in order to avoid this potentially catastrophic loss of confidence. These are captured in a number of associated COA papers that cover the need for:

- Inherent (i.e. it just works) End to End Secure Communications
- Identity and Access Management that can be trusted across organisations, not merely within each organisation
- Device Trust Management mechanisms in which we can be confident
- Commonly Understood Business Impact Levels, to allow effective risk decisions
- Commonly agreed Information Sensitivity Classifications
- Control Stratification that is seen to work
- Enterprise Relationship Management (especially as it pertains to Trust).

It is foundational to this paper that the above must be achieved in an open manner. Open standards are key.

## Background/rationale

An acronym was introduced in the *Collaboration Oriented Architectures*<sup>3</sup> paper, known as PRIDE. This acronym covered the key areas in which Virtual Trust must operate:

PEOPLE, RISK, INFORMATION, DEVICES, ENTERPRISES

One way of looking at this acronym was simply to view the centre 3 terms as connecting People and Enterprises. How well each of the components behave has a bearing on the resulting Trust that can be placed.

Most of the applicable rationale is covered in the *Jericho Forum Commandments* paper and the papers listed in the **Recommendation/Solution** section of this paper.

### The need for open standards: INTEROPERABILITY

The reason that the Internet still uses a set of insecure protocols is because these protocols are de-facto lowest common denominator standards, which are open and free for use. If all systems are to interoperate – regardless of operating system or supplier, and be adopted in a timely manner, then it is essential that protocols must be open and remain royalty free.

## Conclusion

Recognition of the need for mechanisms that support the development and protection of Virtual Trust are key to the continued growth and value of the World Wide Web. It is the position of the Jericho Forum that Governments, Vendors, Users and Consumers all need to co-operate to ensure the development and protection of such behaviours, capabilities, and services as will allow Virtual Trust. This will become even more critical as the full implications of the race toward “Cloud Computing” are realised.

---

<sup>3</sup> Collaboration Oriented Architectures (COA) and COA Framework – papers available at [www.jerichoforum.org/publications](http://www.jerichoforum.org/publications)