Trust in Online Trading Systems

Benjamin Sze Ting Lai

A thesis submitted in partial fulfilment of the requirements for the degree of Master of Science, The University of Auckland, 2003

Abstract

With the emergence of the Internet, electronic commerce and online auction sites we see many systems that are claimed to facilitate the development of trust relationships. However, the authors of these systems rely on various intuitive definitions of trust in the description of their systems, causing confusion among readers.

This thesis clarifies the meaning of trust in an online trading environment. We present a qualitative model that describes the development of trust, reciprocity and reputation in an online trading environment. We validate our model by demonstrating its application to three online trading systems. Our analyses indicate how interpersonal and institutional trust relationships are developed by currently available online trading systems. We hope that future designers, debuggers, analysts, and users of online trading systems will find inspiration and insight from reading this thesis.

Acknowledgements

Writing this thesis has proved to be both a physical and emotional undertaking. It is a physical undertaking in a sense that I have spend my summer holidays sitting in front of the computer writing this thesis while most of my friends are spending theirs holidaying, and it has taken a toll on my physical well being *(my receding hairline!)*. It is an emotional undertaking in a sense that firstly I am on my own for the entire thesis year with regard to the thesis topic – no one else is studying the same topic as I am, secondly as a "single-threaded" creature (that is, I can focus *only* on one task at a time) I get particularly frustrated when I get interrupted with other tasks.

Fortunately I have received a lot of help and guidance throughout the year from various people – physically, academically and emotionally. Without them this thesis would had never eventuated. Therefore I pay my acknowledgements and gratitude to these people for the contributions they have made to this thesis and/or my well being during the course of writing this thesis.

Firstly I would like to thank my supervisor, Clark Thomborson, for giving me the opportunity to work under his supervision. The idea for thesis sprung from a postgraduate project that I undertook under his supervision, and this thesis would not exist if he had not offered me the opportunity to develop the unfinished ideas from the project.

Secondly I would like to thank the entire Computer Science Department at the University of Auckland provided me an excellent environment for writing my thesis *(which surprisingly, was more often the first floor computer laboratories rather than the private desk on the fifth floor)*. Conny Bluefeld notified me of an enrolment fiasco that I managed to get myself into. Ian Watson provided a lot of assistance with my enrolment in the degree *(and notifying me that a short extension is granted automatically!)*. Muharram Khoussainova and Robyn Young provided all the necessary help with the administrative matters *(access cards, keys and alike)*. Keith Johnston and Lei Zhang provided me with all the technical assistance on the department's computer equipment *(physically locking the machine, the MSBlast disaster etc)*.

Thirdly I thank my family for giving me all their moral and material support. Louis (my father) encouraged me into writing this thesis, and provided all the material

assistance. Wendy (my mother) provided a lot of mental encouragement, and the daily necessities *(I miss your cooking already!)*. Being my forever-loving elder sister and confidant, Vivien gave me all that unconditional love that I always appreciate. Always nagging for food and daily strokes with "the glove", caring for Mel (our family cat) is always a relaxing activity at times of extreme boredom or thoughtlessness.

Fourthly I thank my friends whom injected this bland year with colour, laughter, assistance and suggestions: Alan Kan (a MCom(Hons) graduate) provided his moral support and was my role model for completing this thesis. Julia Ho, Georgia Yeung and Bertrand Ngai made my life easier by providing all the laughs and the interesting conversations during this difficult year. Shan Lun actually proof-read this thesis for me in addition to keeping me updated with all his interesting "encounters" *(I hope your "Maori tattoo" tan is getting better).* In addition to all the interesting conversations during our gatherings, Deborah Li gave me a very useful advice of *"writing as though you are speaking to them"*, which helped me through the writing of the Literature Review. Joseph Leung provided all the distractions at the right *(and wrong)* time in the form of computer entertainment, and gave me the one-and-only humorous suggestion *(of sneaking pages from the Karma Sutra into the thesis!)*. In contrast, Ricky Lam always found me at the right time for lunch, conversations, jokes and the occasional arcade games. And Placida Lam's curiosity always caught me off guard and made everything so much more interesting during many of our meal gatherings.

Last but not least, my apologies to anyone that I might have missed – a collective Thank You to you all!!

(Since I have not identified anyone suitable to dedicate this thesis to at the time of writing, I will dedicate this thesis to future students who are interested in the subject)

Table of Contents

List of Figures

List of Tables

1 Introduction

Suppose you want to buy a Nokia 7650 mobile phone. Would you buy it from one of Nokia's authorised retail outlets, from one of eBay's auction listings, or from a random person you have just met in an amusement parlour that happens to have a Nokia 7650 in his pocket?

Buying the phone from a local authorised Nokia outlet seems quite safe, although it is probably the most expensive option. You are trading with a reputable company. You are assured that the phone comes with warranty, that the phone is new, and that you can always send it back to Nokia's service department for repairs if it breaks down.

You might be a little nervous about buying the phone from eBay, especially if you have never used eBay before. By reading eBay's feedback area, you can gain a little information about the other traders, regarding their previous transactions. You don't know whether the phone you get from eBay will have any warranty in your area. You don't know whether the phone is new or is a second-hand. You might have to send it to third-party repair shops if it breaks down.

You might be very cautious about buying the phone off that random person you've just met in an amusement parlour. You have no idea who he is. You are not sure whether the phone comes with any remaining warranty. You don't even know whether he bought his phone or he happened to stumble across it on the street or even stole it.

In our hypothetical scenario described above, we have put more trust in Nokia's authorised retail outlet than in a trader in eBay, and we have trusted eBay more than the random person from the amusement parlour. In the first case we trust an authorised Nokia retailer because Nokia's reputation is reflected in the phone outlet's branding. A reputable brand mark on a retailer, such as "Nokia authorised dealer", assures us of the quality of our purchases and after-sale services. In the second case we require more information about an eBay trader before we develop sufficient trust to trade with him. Such assurances may be obtained through other traders' feedback about the trader in question. For the random person in the amusement parlour we will need a lot of assurances, for example a character testimonial from someone we both know, before we would trust that he is not trying to sell us stolen goods.

We make trusting choices everyday, as it is a "basic fact of life" [Luhmann 1979]. For example, we might trust that drivers will stop at the zebra crossing where we want to cross the road. However trust is different to certainty: each time we put our trust in something we are also putting ourselves at risk – the risk that the thing we are trusting is not going to be realised. In the zebra crossing scenario, we are putting ourselves at the risk that the driver might not stop at the zebra crossing for us.

This thesis is concerned with trust in a specific scenario: online trading systems. A lot of research has been done on the topic of trust in various disciplines, and there are a lot of technologies and mechanisms that claim to promote trust in an online trading environment. We have discovered that many authors fail to define the term *Trust* for their systems or pieces of research and that there are many intuitive definitions for the term. This makes it difficult to develop a clear understanding of trust-related research [McKnight 2001]. In addition some pieces of research are concerned only with a static one-off analysis of trust at one point in an E-Commerce scenario [Ahuja 2000, Shneiderman 2000], as opposed to a dynamic analysis of trust relationships during the different phases of an E-Commerce transaction [Mui 2002]. Lastly we have observed two ways system facilitate the development of trust: they either assist the development of trust among their users through internal mechanisms built into the systems themselves, or they rely on external (often informal) mechanisms for the development of trust among their users.

This thesis develops a methodology for analysing how an online trading system facilitates the development of trust relationships. We approach the problem by firstly clarifying the definition of *Trust* and its related terms in an online trading environment, then we developing our own qualitative, analysis-oriented trust model, and lastly using this model to analyse some of the online trading systems that are currently available or proposed. We hope that designers, debuggers, analysts, and users of online trading systems will benefit from our trust model and the analyses we have conducted using the model.

We organise our thesis in the following manner: Chapter 2 is a survey of literatures from various disciplines that discussed the concept of trust, from (social) psychology, sociology, to electronic commerce, software security and computer science. Our main contributions start at Chapter 3, where we present our qualitative model for trust developments, along with the modelling rationales and definitions of the fundamental terms used in our model. In Chapter 4 we present our analysis of

three online trading systems using the trust model we have developed in Chapter 3. We summarise our findings and offer our conclusions about our trust model and the systems that we have analysed using our trust model in Chapter 5, followed by the Appendix in Chapter 6, which contains detailed information about the modelling of messages both in the process of developing our trust model, and in the process of analysing the various online trading systems.

Although this chapter is one of the first bits our readers read, it was one of the last things we wrote. Yes we will bore our readers to death with our literature review. We will haunt our readers with all the mumbo-jumbo that we have created for our model. Lastly we will terrify our readers with all the bullet points, Visio diagrams and Excel tables we have found worthy of incorporating into the analysis section of this thesis. And by the way, some random person did actually try to sell a Nokia 7650 mobile phone to the author at an amusement parlour.

2 Literature Review

Many researchers from various fields have investigated the notion of trust. Their findings are orthogonal to each other, making it difficult to come up with a unified notion of trust. Here we present a summary of the previous findings.

We have identified several major difficulties faced by prior researchers. Firstly, as mentioned in Chapter 1, "trust" is a vague term to define; it has more definitions than similar terms such as *confidence*, *cooperation* and *predictable* [McKnight 2001].

Secondly everybody has their own perception of what trust is [Marsh 1994, McKnight 2001]. Researchers come up with their own definitions of trust and vigorously defend their definitions for their pieces of research [McKnight 2001]. For example, in operating systems "trust" refers to access control, especially for classified or other sensitive information [DoD 1985], while in digital certificates "trust" implies identity verification and non-repudiation, and in Electronic Commerce "trust" is typically associated with the safeguarding of personal and credit card details.

Thirdly few have tried reconciling various types of trust into a single construct [McKnight 2001], and are faced with difficulties due to conflicting views among disciplines. For example, sociologists [Barber 1983, Luhmann 1979] argue that trust cannot be reduced into personality variables [McKnight 2001], in contradiction to the views of social psychologists [Deutch 1973, Rempel 1985].

The scope of this literature review is as interdisciplinary as possible, despite the author's limited educational background in social psychology, sociology, philosophy and commerce. We pay attention to topic areas in the computing discipline such as digital certificates, model formulations and electronic commerce.

Morton Deutch [Deutch 1973] is a social psychologist who carefully investigated the notion of trust. In his work, *The Resolution of Conflict*, he provides a classification of the circumstances in which a trust decision could be made. Such circumstances include situations of despair, social conformity, innocence, impulsiveness, virtue, masochism, faith, risk-taking, and confidence. Although he provided no definition for the term "trust" he provided a definition for the term "trusting choice". With his focus in trust as confidence, he presents a series of hypotheses, with assumptions which are rooted in psychology [Marsh 1994].

Bernard Barber [Barber 1983] is a sociologist who is concerned with the vagueness in the definition of the term trust and its over-liberal usage. He attempted to provide a concrete definition for the term in his work, *The Logic and Limits of Trust*. In his work, he regards trust as "expectations that actors have of one another" [Barber 1983]. He looked into three particular types of expectations, which will be discussed in section 2.3 of this chapter.

Niklas Luhmann [Luhmann 1979, Luhmann 1988] is a German sociologist who proposed his formalism on trust at around the same time as Barber. In his work he suggests trust as a means to reduce complexity of society, and also as a means to handle risk. Luhmann also suggests that "distrust" is a *qualitative opposite* of "trust", that is, "distrust" is not "a lack of trust" but rather is a form of "negative trust".

Diego Gambetta [Gambetta 1988] gathered a collection of reports from various fields that looked into the topic under the title *Trust* [Gambetta 1988]. In his concluding essay he questioned whether trust is a rational choice, i.e. can we trust the notion of trust. He provides a definition for the term trust in his concluding essay, which views trust as a probability.

Various researchers have proposed mathematical models to formalise the concept of trust [Abdul-Rahman 1997, Abdul-Rahman 2000, Aberer 2000, Marsh 1994 and Mui 2001], and many have developed technologies and systems to support the development of trust in online communities.

The remainder of this chapter is organised as follows: firstly we discuss the various social levels of trust that researchers have recognised as existing in society. Then we discuss various research efforts that focus on qualitative aspects of trust. We then discuss some of the research efforts that focus on the quantitative aspect of trust, which includes various descriptive models concerning the progressing stages of trust, and various mathematical trust models. And lastly we discuss the various security strategies and pieces of technologies that researchers have developed to support the development of trust relationships and to reinforce existing trust relationships in the online environment.

2.1 Dictionary Definitions

We first explored the dictionary meanings of the term trust and related terms that are used by other researchers [Deutch 1973, Barber 1983, Mui 2001] such as confidence, expectation, reputation, and reciprocity. The online version of The Oxford

English Dictionary [Oxford 2003] was used to look up these definitions. There are numerous definitions for those terms, and the ones that are relevant to our research are as follows:

Trust (as a noun):

1. (a) Confidence in or reliance on some quality or attribute of a person or thing, or the truth of a statement.
   (b) ***Take on*** or ***upon trust (receive, take up in trust, take up upon trust)***, to accept or give credit to without investigation or evidence.
2. Confident expectation of something; hope
3. The quality of being trustworthy; fidelity, reliability; loyalty, trustiness. Now *rare*.
4. (a) The condition of having confidence reposed in one, or of being entrusted with something; esp. in the phrases ***in trust***, ***to one's trust***, ***under trust.***
   (b) The obligation or responsibility imposed on one in whom confidence is placed or authority is vested, or who has given an undertaking of fidelity.

Confidence (noun):

1. The mental attitude of trusting in or relying on a person or thing; firm trust, reliance, faith.
2. The feeling sure or certain of a fact or issue; assurance, certitude; assured expectation.
3. Assurance, boldness, fearlessness, arising from reliance (on oneself, on circumstances, on divine support, etc.).
4. In a bad sense: Assurance based on insufficient or improper grounds; excess of assurance, overboldness, hardihood, presumption, impudence.

Expectation (noun):

1. The action of mentally looking for some one to come, forecasting something to happen, or anticipating something to be received; anticipation; a preconceived idea or opinion with regard to what will take place.
2. The degree of probability of the occurrence of any contingent event.

Reputation (noun):

1. (a) Opinion, supposition; also, the opinion or view *of* one about something.
   (b) Account or estimation *of* a thing
2. The common or general estimate of a person with respect to character or other qualities; the relative estimation or esteem in which a person or thing is held.
3. The condition, quality, or fact, of being highly regarded or esteemed; credit, note, or distinction; also, respectability, good report.
4. The honour or credit of a particular person or thing; one's good name, good report, or fame in general.

Reciprocity (noun):

1. The state or condition of being reciprocal; a state or relationship in which there is mutual action, influence, giving and taking, correspondence, etc., between two parties or things;

From the dictionary definitions we identify the properties that are often associated the term trust to be that of confidence, reliance, and without deep investigation or strong evidence.

2.2 Social Levels of Trust

After reading a dozen or so articles on trust from disciplines including (social) psychology, sociology and computer science, it was observed that there are different objects that we trust regardless of the situation. An overview of those objects will be provided before going into the different social levels of trust that result from trusting those various objects.

Often the first object that we place our trust on is ourselves; this personal level of trust is usually in isolation and is one of the factors why two people might make a different trust decision given the same situation.

The second type of object that we place our trust upon is another individual; trust in this level is placed on one other individual and the level of trust we place upon each individual will differ.

The third type of object that we place our trust upon is an organisation. An organisation usually has some sort of membership and branding. We often place trust in an organisation at a general level, for we often have little knowledge about the components that make up that organisation.

Many researchers focus on a trust model that has three levels of trust based on those three different objects we place our trust on, as it is believed that there are distinctions among a person's trust in his own self, a person's trust in another individual and a person's trust in a body of people (e.g. an institution).

2.2.1 Individual Trust

Individual Trust, or "Dispositional Trust", focuses on a person's personality characteristics being a factor in making a trust-related decision. This is in essence a person's general trusting attitude, and is independent of the contexts in which trust decisions are made [Abdul-Rahman 2000].

As each individual's personalities and experiences are inherently different, their trusting attitude for a particular situation will be different. Deutch [Deutch 1973] includes an element that is a "personal security level", that varies among individuals in his series of hypothesises for trust between individuals. Rempel et al [Rempel

1985] states that an individual's trust develops from his past experiences and previous interactions.

2.2.2 Interpersonal Trust

Interpersonal Trust, or "Relationship Trust", is a social level of trust that focuses on the factors that create or destroy trust relationships between individuals. Interpersonal Trust has been researched extensively by (social) psychologists, who approach trust in various contexts. Two of the more popular contexts are to approach trust as confidence and as expectations a person has in another individual. Deutch [Deutch 1973] took on a view of trust as confidence when he worked on the topic. Rempel et al [Rempel 1985] regarded trust in their model for trust in close relationships as "a generalised expectation related to the subjective probability an individual assigns to the occurrence of some set of future events".

The conceptualisations of Interpersonal Trust often involve factors such as the trusted party's past behaviour. In Rempel et al's model of trust [Rempel 1985] consistency of recurrent behaviour is a factor for the initial stages of the development of trust relationships. Mui et al [Mui 2001], in their quantitative model for trust, regards trust to be based on the history of past encounters.

2.2.3 Organisational Trust

Organisational Trust is the approach taken by sociologists in their research into trust. Organisational Trust is a social level of trust that focuses on the development of trust in an individual with respect to other groups of people. We identified two types of Organisational Trust, and they are Institutional Trust and System Trust.

The first type of Organisational Trust is Institutional Trust. An institution is an organisation of people, with recognisable properties such as membership and branding. For example, people can recognise students from a particular school by the uniform they wear.

Institutional Trust is a social level of trust that focuses on the development of trust between individuals and institutions. It is believed that individuals generalise their personal trust in institutions, when they do not have much familiarity with the people that make up those institutions [Kini 1998].

The second type of Organisational Trust is System Trust. A system is an organisation of people, institutions and technologies, with a recognisable interface.

For example, the monetary system is an organisation of people, the government, banking institutions and other institutions, with a common interface of a currency (in New Zealand it will be the New Zealand Dollar).

In System Trust a person's trust does not lie in another person or in an institution, but rather it is placed in the perceived properties of the system in which the trusting and the trusted parties operate on [Abdul-Rahman 2000]. System Trust can only be built up by "continual, affirmative experience" in interacting with the system in question [Luhmann 1979]. The initial trust in a system is not discussed in the literature we surveyed, however it seems reasonable to assume that it is achieved by association with Interpersonal Trust ("word of mouth") or Institutional Trust (perceived "branding"), by coercion (i.e. monopoly or in situations where there are no perceived alternatives), or by attraction (reward of some sort for initial use).

Researchers of Organisational Trust assert that trust is a "phenomenon of social, structural and cultural variables" [Barber 1983], as opposed to a function of individual characteristics as suggested by social psychologists [Barber 1983]. Luhmann argues that attempts to reduce the social sphere into individual personality variables by social psychologists are the reason why they cannot provide a clear explanation for *why trusting choices are made* [Luhmann 1979, Page 9, Note 10].

2.3 Qualitative Trust

In our exploration in existing literatures on trust we have found works that look into various qualities of trust. The authors include Bernard Barber [Barber 1983], who formulated trust as expectations, Audun Jøsang [Jøsang 1997] and Mui et al [Mui 2002] who proposed qualitative trust models for computing systems.

2.3.1 Expectations of Trust

While trust can be viewed as having various characteristics, such as despair and virtue, Bernard Barber and many other researchers have treated trust as an expectation.

Barber offers three definitions of trust in his monograph [Barber 1983]. He does however make it clear that trust is some form of expectation about some person or thing, regarding future, fiduciary obligations and responsibilities [Barber 1983]. His three expectations of trust that "involved some of the fundamental meanings of trust" are listed below:

1. Expectation of the persistence and fulfilment of the natural and the moral social orders.
2. Expectation of "technically competent role performance" from those we interact in social relationships and systems.
3. Expectation that partners in interaction will carry out their fiduciary obligations and responsibilities, that is, their duties in certain situation to place others' interests before their own.

[Barber 1983, page 9]

While these expectations may sound misplaced or misdirected if we consider trust in interpersonal relationships (such as friendships or romantic relationships), they are sensible if we consider trust in institutions (such as the government and professional institutes). According to Barber's expectations we can expect professionals to act in a responsible manner and not to exploit or attempt to blind us with their technical expertise in order to pursue their own personal agendas.

In a general sense, Barber suggests that trust is an expectation that the natural, physical, biological and social order will endure and be fulfilled to a certain extent. He puts particular emphasis on trust as an expectation in moral social order, asserting that trust is a fundamental ingredient in all social relationships.

Barber also suggests that there are two specific expectations of trust. The first specific expectation is the expectation of technically competent role performance. This is evident when we place our trust in surgeons to perform operations well, and when we place our trust in builders to build houses with good workmanship. The second specific expectation is the expectation of fiduciary obligations and responsibilities being fulfilled. That is, we expect people with moral obligations and responsibilities to fulfil those accordingly, and to place our interests before their own. This is evident in the legal profession where lawyers have the obligation to act in their clients' best interests, regardless of whether they may have conflicting agendas.

2.3.2 Qualitative Trust Models

In addition to Quantitative Trust Models (to be discussed in Section 2.3.2) that attempts to assess the amount of trust an agent has, there have been research efforts into "qualitative" trust models that describe the general message flow between the participants. While some of these qualitative trust models are intended to be purely theoretical models [Jøsang 1997], some of them are actually simple models that are intended to be an intermediate tool in the process of coming up with a quantitative trust model [Mui 2002].

Audun Jøsang [Jøsang 1997] proposed a theoretical trust model in his work, *The right type of trust for distributed systems*. In this work he distinguished two kinds of entities: the passionate entity, such as a human being, that has the free will to choose between benevolent and malicious behaviours; and the rational entity, such as a computer system, that does not have the choice between benevolent or malicious behaviours. While rational entities cannot be benevolent or malicious, they will resist attempts of malicious manipulation by an external, passionate, and malicious entity.

Mui et al [Mui 2002] introduced a qualitative trust model as part of their model rationale for their quantitative trust model. There are three fundamental elements in their qualitative trust model: *Reciprocity* which deals with the exchange of deeds between agents, *Reputation* which deals with the perception of an agent's intentions through its past behaviours, and *Trust* which is a subjective expectation of an agent's future behaviour. They suggest that these three elements have some sort of influence among each other, and that the "levels" of each of the elements would change as more interactions among agents are taken place. Mui et al's qualitative trust model will be discussed in detail in the next chapter, for we have adopted it as a foundation of our research.

2.4 Amount of Trust

There have been research efforts conducted to investigate the progressive stages that a person undertakes in order to place trust in another entity. While each of the models has their merits and shortcomings we have identified some similarities among the models. We here present summaries and short comparisons of the three pieces of research we found to be of most interest among our readings: Rempel et al's model [Rempel 1985] which is based in social psychology, Fung and Lee's model [Fung 1999] and Cheskin Research's model [Cheskin 1999] which is based around electronic commerce.

2.4.1 Predictability, Dependability and Faith

Rempel et al [Rempel 1985] proposed a three-stage model for trust in close relationships. In this model the three stages are labelled predictability, dependability and faith, with increasing levels of abstraction in terms of attributes between the stages.

The first, and the most specific and concrete stage of trust is predictability. In this stage the factors that influence one's perception of another's trustworthiness

include consistent recurrent behaviour and stability of the social environment. In addition knowledge about the existence of reinforcements and restraints of behaviour will enhance one's ability to predict another person's future behaviour. Therefore to an extent predictability is a type of reinforcement mechanism whereby predictions of an individual's future behaviour relies heavily on that individual's consistent responses made in the past.

The second stage in Rempel et al's model of trust is dependability. Like predictability, dependability also takes past experiences and reliability of previous evidence into consideration, but unlike predictability where evaluations are made on a person's future behaviour based on previous specific behaviours, in the stage of dependability evaluations are made on a person's personality attributes based on his previous behaviour. Trust in this stage is placed on a person's perceived attributes rather than his specific behaviour. While trust evaluations made in the stage of predictability serves as a foundation for building trust relationships in the stage of dependability, significant trust developments in the stage of dependability will depend on one's willingness to expose himself to risks and the possibility of betrayal by the trustee.

The third stage of trust, in Rempel et al's model, is faith. This stage of trust covers one's trust in the trustee that is not "deeply rooted" in past experiences. The focus in the stage of faith goes beyond specific behaviour and personal attributes – it concerns itself more with a person's motives and intentions. While predictability and dependability are somewhat necessary for the development of faith to a certain extent, they are not the only factors that influence one's trust in another in this stage.

2.4.2 No Trust, Formal Trust and Informal Trust

Cheskin Research, in association with Studio Archetype/Sapient, conducted research into the nature of trust in E-Commerce in 1999 [Cheskin 1999]. In this research they propose a model which they suggest is the way trust is developed in an E-Commerce environment.

Cheskin's model of E-Commerce trust has three distinct stages: *No Trust*, *Formal Trust* and *Informal Trust*. Initially in the No Trust stage the consumers are new to E-Commerce and they perceive the web to be in some sort of chaos, where information is vulnerable to interception, and technology is unreliable. The desire for control emerges as the result of the consumers' perceptions of chaos in the web.

Once the consumers become familiar with the web we proceed into the second stage in Cheskin's model of E-Commerce trust: Formal Trust. In this stage consumers are aware of the technologies or third party seals that are designed to promote a secure environment for E-Commerce. The consumers would only participate in transactions with an E-Commerce website if such technologies and/or third party seals are present and being used. As transactions accumulate we proceed into the third stage of Informal Trust under Cheskin's model, where the consumers are confident in their expectation of a specific E-Commerce site, and willing to place their trust in it and participate in more informal transactions.

2.4.3 Fung and Lee's EC-Trust Development Life Cycle

Fung and Lee [Fung 1999] proposed a trust model specifically for electronic commerce, which they called *The EC-Trust Development Life-cycle*, as illustrated in Figure 2-1. In their trust development life-cycle there are several distinct processes grouped in two stages. These processes are intended to show the main flow of events that lead either to distrust or to a firm trust relationship between the consumer and the merchant.

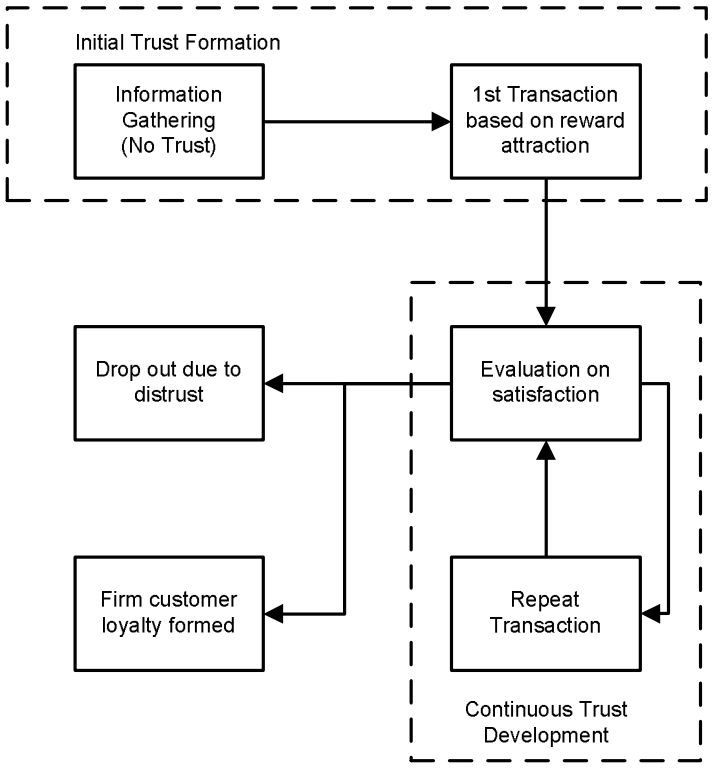


Figure 2-1 The EC-Trust Development Life-cycle [Fung 1997]

From the description of the model it is noted that there are similarities between the EC-Trust Development Life-cycle and Cheskin Research's trust model [Cheskin 1999]. They both have a "No Trust" stage where the consumer gathers information about the electronic merchant. Cheskin's model has an "Informal Trust" level, which is similar to the formation of firm customer loyalty in Fung and Lee's model. One ambiguity in Fung and Lee's model is whether or not the existence of reward attraction is really necessary for the first transaction between the consumer and the electronic merchant to occur; a related question with regard to Fung and Lee's model is whether the "First Transaction based on reward attraction" process is the only entry point to the second stage of the model.

2.4.4 Quantitative Trust Models

A number of researchers have formalised the concept of trust into mathematically sound models. Such "Quantitative Trust Models" include those by Abdul-Rahman and Hailes [Abdul-Rahman 1997, Abdul-Rahman 2000], Aberer and Despotovic [Aberer 2001], Marsh [Marsh 1994], and Mui et al [Mui 2002].

One of the first studies that looked into formalising the abstract notion of trust into some concrete notion that can be used in computing was conducted by Marsh [Marsh 1994]. His trust model is rooted in sociological foundations, and has been critiqued and reviewed by many researchers [Abdul-Rahman 2000, Aberer 2001, Mui 2002]. One major shortcoming recognised by these researchers is that Marsh attempts to include all aspects of social trust into his model. This introduces a large number of variables into his model. As a result his model is so large and complex it cannot be easily implemented in today's systems [Abdul-Rahman 2000, Aberer 2001]. Secondly trust in his model was presented as real numbers between -1 and 1, and the model encounters problems when dealing with extreme values and at 0 [Mui 2002].

Abdul-Rahman and Hailes [Abdul-Rahman 2000] proposed a model that is also based on sociological principles. In this model the concept of trust was divided into *direct* trust and *recommender* trust. While direct trust is concerned with an agent's belief in another agent's trustworthiness within a certain context, recommender trust focuses on an agent belief in another agent's trustworthiness in giving recommendations about other agents within a certain context. Instead of using real numbers as in Marsh's model of trust, in Abdul-Rahman and Hailes's model there are four distinct values: "Very Trustworthy", "Trustworthy", "Untrustworthy", and

"Very Untrustworthy". The main problem in this approach is that every agent in the system must keep a rather large and complex data structure to represent the knowledge it knows about other agents in the system. Updating this data structure can be a time consuming and labour-intensive work in real world situations [Aberer 2001].

Aberer and Despotovic [Aberer 2001] proposed a model for managing trust in a peer to peer computing environment. In this model their goal was to derive a model that provides information for agents to make their subjective trust assessments despite the limitations of data management in an agent-based system. To accomplish the goal they firstly simplified the concept trust to deal with only one context (they claim that context considerations can be easily integrated into the model), and secondly they made an assumption that agents in the system are trustworthy unless there is evidence that proves the contrary. As the result rather than collecting and propagating positive experiences with an agent their model collects and propagates complaints that other agents made about a particular agent. While their model does achieve the goal of efficient data management of trust information in a peer to peer environment, the modelling of trust in an optimistic matter might have its shortcomings. The collection and propagation of complaints alone will only distinguish the untrustworthy agents from the rest, and distinguish the varying degrees of untrustworthiness among the untrustworthy agents; unless positive information (such as appraisals) is collected, there is no way to distinguish varying degrees of trustworthiness among the trustworthy agents.

2.4.5 Discussion on the Three Models for the Stages of Trust

We find that the three models of progressions in trust by Cheskin Research, Rempel et al and Fung and Lee have various similarities and orthogonality. Thus we conducted comparisons among the three trust models, and diagrammed the results in Figure 2-2. The directions of the lines indicate the degrees in which the trust models complement or are orthogonal to each other – the closer the direction of the lines the more the corresponding trust models complement each other. The length and position of the line segments indicate the level of trust the various stages of the trust models have.

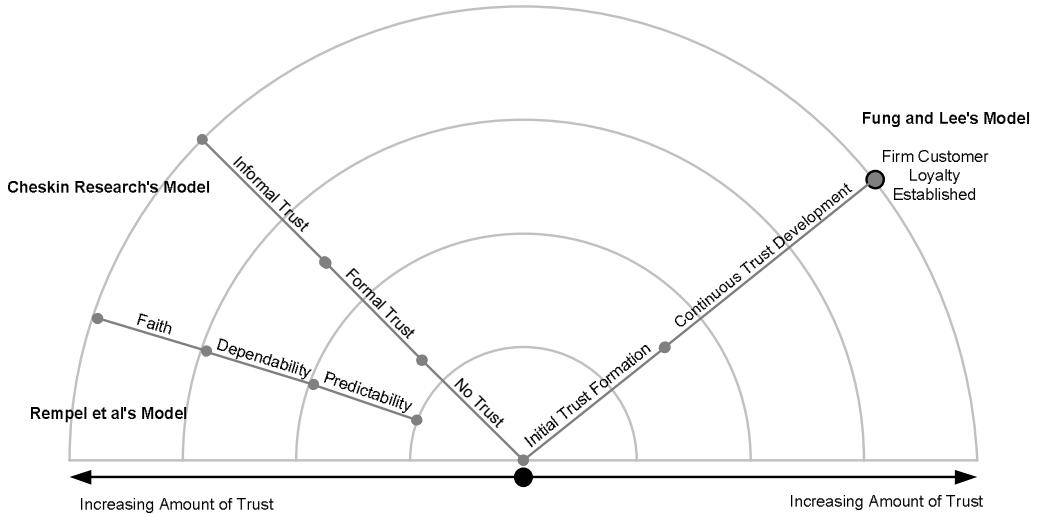


Figure 2-2 Comparison between Rempel et al, Fung and Lee and Cheskin Research's model for progressions in trust

Comparing Rempel et al's model of progressions in trust with Cheskin Research's model, we identify some similarities and overlaps between the models. There isn't a functional equivalent of Cheskin's "No Trust" stage in Rempel et al's model. There are similarities in Cheskin's second ("Formal Trust") stage with the first (Predictability) stage in Rempel et al's model technologies such as SSL encryption that are relied upon in Cheskin's "Formal Trust" stage are the reinforcements and restraint of behaviour that will enhance one's prediction about future behaviours in Rempel et al's Predictability stage.

The third ("Informal Trust") stage in Cheskin's model is similar to the second (Dependability) stage in Rempel et al's model as reinforcements and restraint of behaviour becomes less of a governing factor in trust development compared with the first ("Formal Trust") stage in Cheskin's model and the first ("Predictability") stage in Rempel et al's model, and that trust development in the "Informal Trust" and "Dependability" stages is based on attributes and characteristics in the trusted party rather than specific behaviours. It is noted that Cheskin's "Informal Trust" stage does not correspond to Rempel et al's Dependability stage in its entirety, as there is still a significant amount of reliance on reinforcements in the "Informal Trust" stage in terms of technologies and trusted seal marks. There is no stage in Cheskin's model that corresponds fully to the Faith stage in Rempel et al's model.

We also identify some similarities and overlaps between Cheskin Research's trust model and Fung and Lee's trust model. In first stages of their trust model ("No

Trust" in Cheskin's model and "Initial Trust Formation" in Fung and Lee's model) both are concerned with some form of explicit reassurance. In Cheskin's trust model it is the reassurance of control, especially the control of personal information. In Fung and Lee's model it is the reassurance of the accuracy of the information.

We identify that the second stage ("Continuous Trust Development") in Fung and Lee's trust model spans across the second and third ("Formal Trust" and "Informal Trust") stages in Cheskin Research's model. The second stage in Fung and Lee's model is concerned with the development of trust between the consumer and the E-Commerce website through repeating interaction, which is the method of developing trust throughout the second and third stage of Cheskin Research's model. We identify that the third stage ("Firm Customer Loyalty Established") in Fung and Lee's model corresponds to the very advanced phase in the third ("Informal Trust") stage of Cheskin's trust model.

2.5 Technologies that Support Trust

Since the 1970's researchers have been looking into computer security from the encryption of messages in the early days to the more sophisticated mechanisms and technologies that are employed today. We will look into the various technologies that have been proposed or deployed to support the development of trust relationships on the internet. They range from traditional security mechanisms such as encryption and secure communication channels, to people-oriented online feedback systems, seals of approval, and escrow agents, and even alternate dispute resolution systems.

2.5.1 Seals of Approval

Seals of Approvals are symbols designed to re-assure a website's visitor that either security has been established [Cheskin 1999], or a particular E-Commerce website's business policies and practices have met a set of requirements [Patton 2001]. Such requirements are usually listed on the Seals of Approvals' websites either in summary or in detailed form [TRUSTe 2003, BBBOnline 2003]. Some Seals of Approval require the E-Commerce website's policies and practices be inspected by the organisation that is responsible for issuing the Seal.

There are a number of organisations that issue such Seals of Approval. TRUSTe provides a range of Seals for privacy assurances, from the general privacy seals to privacy seals that target child-themed websites and health internet sites [TRUSTe 2003]. BBBOnline issues two types of Seals: a privacy seal similar to ones

offered by TRUSTe, and a reliability seal that certifies that the E-Commerce website meets the requirements set out by BBBOnline, which includes abiding by the BBB Code of Online Business Practices and the BBB Code of Advertising, as well as providing a channel for dispute resolution [BBBOnline 2003]. In contrast to TRUSTe or BBBOnline, Verisign offers Seals that focus primarily on certifying that confidential transactions on certified sites are secured by SSL encryption [Verisign 2003].

In Cheskin's study in E-Commerce Trust in 1999 [Cheskin 1999], only one third of the respondents recognised the Verisign symbol, but over one-half of those people who do know the symbol said that it would increase their trust in an E-Commerce website. A subsequent study [Cheskin 2000a] found that while there is an increase in the number people in the US who both have seen such Seals of Approval and also perceive an increase in trust for the E-Commerce website that has such Seals, there was little increase in trust for respondents in Latin America and Brazil, where such Seals of Approval are not well known. Thus while Seals of Approvals do improve consumers' perceptions about an E-Commerce website's trustworthiness, they are only effective if the seals are well-known to them.

2.5.2 Reputation Systems

Reputation Systems are essentially feedback systems which enable participating parties in a transaction to provide feedback on each other [Resnick 2000]. The feedback usually consists of a rating (positive, neutral or negative) and comments, and these ratings and comments can be aggregated to represent the "reputation" of a user in the system.

The original design goals of reputation systems are to assist users in deciding who to trust in a system, to encourage trustworthy behaviour, and to discourage and deter untrustworthy or dishonest people from participating in the system where the reputation system is implemented [Resnick 2000].

Although they were designed be implemented as part of an E-Commerce system, reputation systems are also used for product review purposes. An example of a reputation system is the trader feedback system used in eBay [eBay 2004a]. The product feedback system used at Amazon.com is an example of reputation systems being used to provide product reviews by users [Amazon.com 2003].

One of the design goals of reputation systems is to encourage trustworthy behaviour in the E-Commerce system where the reputation system is implemented. The argument is that the aggregation of positive feedback on a particular user X in the system will give other users a perception that user X is trustworthy, thus encouraging other users to conduct transactions with user X in the future.

One of the weaknesses of reputation systems is the fact that reputation ratings are heavily dependent on the identification of users by their aliases. If the association between an online alias and the physical person it represent is relatively weak, a user can essentially "reset" his reputation in a system by changing his alias through reregistering with the system.

As a result some E-Commerce systems require users to provide some proof of identity, such as a credit card number in eBay, or a home phone number in TradeMe (http://www.trademe.co.nz/), as part of the registration process, while some researchers propose the use of real names or "once-in-a-lifetime-pseudonyms" in reputation systems [Resnick 2000].

There are also difficulties in eliciting feedback: users in the system may not provide any feedback at all; negative feedback is difficult to elicit; and there are difficulties in ensuring that feedback is fair and honest [Resnick 2000]. Difficulties in ensuring fair and honest feedback provide the opportunity for conspiring users to compromise the system by giving unfair ratings or by positively or negatively discriminate against users in the system [Dellarocas 2000].

To compromise a reputation system's ability to provide accurate information through eliciting unfair ratings, an "attacker" may collude with other users of the system in order to either give the victim an unfairly low rating ("bad-mouthing"), or to give the attacker an unfairly high rating ("ballot stuffing"). Similarly to compromise a reputation system through discrimination the attacker may positively or negatively discriminate against other users in the system, thus giving him a better reputation rating in the system. An attack may positively discriminate against others by providing exceptionally good service to a few individuals and average service to the others, or he may negatively discriminate against other users by providing good service to all but a few individuals that the attacker dislike.

2.5.3 Label Bureaus

Similar to reputation systems, Label Bureaus are also feedback systems, but they contain ratings by independent third parties, rather than parties directly involved in an online activity [Shepherd 2001].

Label bureaus function as follows. Initially an object X (such as a user, a website, or a digital object) requires some sort of classification. An entry is made in the label bureau for object X with an initial description provided by its author; authorised users (such as independent reviewing agencies) may attach labels - aspects which can be classified and rated - to object X's entry. They may also provide comments and ratings to labels for object X. This information may then be distributed to other users of the system across the internet.

Label bureaus were originally developed for content filtering purposes [Palme 1997], as Trusted Third Parties that served as storage and distribution points for labels and ratings that are used in web browsers to filter out objectionable content for selected audiences. For example, a label bureau may distribute rating information on websites for web browsers to filter out sexually explicit or graphically violent content for children.

The use of label bureau as a trust management system for E-Commerce websites was proposed by Shepherd et al in [Shepherd 2001]. They argued that while Seals of Approval provide a rating for a particular E-Commerce website which indicates to the consumers that the website has met a certain criteria those seals represent (such as requirements in privacy policies and business practices), that rating is a summarisation of different dimensions in which the site was evaluated on. They argued that with Seals of Approval the consumers may be unaware of things such as the nature and scope of those rating dimensions, the allowable values for each of the dimensions, and the actual value assigned for each individual dimension. They suggested that using label bureaus would be a better approach in communicating trust information about an E-Commerce site to consumers than Seals of Approval, as with label bureaus the consumers are able to enquire about the dimensions an E-Commerce website's summarised rating was based on, the allowable values for each dimension, and the assigned rating for each individual dimension. In addition consumers are able to look in multiple label bureaus for ratings on a particular E-Commerce website if a particular label bureau does not have the rating for a particular dimension. Shepherd et al proposed an algorithm of aggregating ratings in multiple dimensions from

multiple label bureaus into a single rating using weights; they claim that the users are able to customise those weights to suit their own preferences.

The first advantage of label bureaus is its ability to provide ratings of an E-Commerce website in multiple dimensions. As a result, users of label bureaus have more information in deciding which E-Commerce website they would trust. Secondly the availability of multiple label bureaus provides users with ratings and opinions in an independent and unbiased manner.

Although we have not come across literatures that discuss the disadvantages of label bureaus, we identify that one possible issue with label bureaus lies in the fact that different label bureaus may have their own classifications of dimensions in which ratings are provided. Firstly those dimensions may overlap each other - hence reconciling those dimensions across label bureaus for rating aggregation is a non-trivial and possibly difficult task. Secondly as a result of the complexities from the overlapping of dimension across label bureaus, assignments of weights to dimensions for rating aggregation will be such a difficult task that only the most competent users of the system will be able to take advantage of the feature.

A trust management system that is a hybrid of reputation system and label bureau was proposed by Daignault et al in [Daignault 2002]. This hybrid system holds two kinds of labels. The first kind of labels is similar to the labels in traditional Label Bureaus, and it stores comments and ratings made by third parties such as independent rating agencies. The second kind of labels stores computed summarisations of ratings that are captured by an associated Reputation System, and those labels may store ratings that are grouped by various categories.

While this hybrid system is fully capable of capturing ratings from all possible sources (i.e. users, independent rating agencies and alike), one possible issue with this approach would be the increased requirements in terms of processing power and data management while running this hybrid system – it is equivalent to running both a label bureau and a reputation system.

2.5.4 Security Strategies

The common security goals for E-Commerce systems are to ensure that information transmitted between the consumer and the merchant is not intercepted during a transaction, to ensure that the identity of the client is who he/she claims to

be, and to protect any sensitive information stored in the servers of the E-Commerce Systems.

While the security strategies mentioned above may convince the users to believe that the system is trustworthy, it does not necessarily mean that the person or organisation that uses the system is trustworthy. Security strategies do not lead to trust relationships on their own; they reinforce existing trust relationships [Gollmann 2002].

2.5.4.1 Secure Socket Layer (SSL) and Encryption

One obvious and common security strategy used in E-Commerce to reduce the chance of compromising sensitive data in the event of interception attacks is the use of encryption over the transmission channel. Secure Socket Layer (SSL) with a choice of encryption algorithm is a popular combination for E-Commerce systems. Usually the E-Commerce system would initiate a SSL connection with its users in parts of the transaction where sensitive data will be transmitted, such as the stage when the user enters in his/her credit card details. In theory, any encrypted data intercepted would be unreadable by the attacker; if the attacker attempts to decrypt the data, the time required to decrypt the data will be infeasible for the capabilities of modern computers. Even if the attacker manages to decrypt the data, the decrypted information would not be timely enough for it to have any tangible value.

The strength of security provided by SSL is partly dependent on the encryption algorithm used. SSL does not have a built-in encryption algorithm; instead it provides a standard for exchanging data using one of the available encryption algorithms. There are many encryption algorithms that can be used for encryption in SSL, the commonly used algorithms include DES (Data Encryption Standard), MD5 (Message Digest Algorithm), RC2/RC4 (Rivest's Stream Ciphers), RSA (Rivest, Shamir and Adleman's Public Key encryption algorithm) and Triple-DES (DES applied three times).

One possible attack on SSL is to intercept the encrypted data and attempt to recover the decryption key. So far the obvious way to recover the decryption key is to conduct a brute-force search in the key space, which requires tremendous amount of time even with the capabilities of the computers available today. There had been competitions held by RSA Security in decrypting a secret message given only its DES-encrypted form [RSA-Security 1997], and within two years since 1997 when the

first challenge was issued the time taken to decrypt the message had reduced from 96 days to less than 24 hours [RSA-Security 1998]. Although those efforts involved a huge amount of cooperation with thousands of computers, it is only time before the emergence of powerful computer hardware that can "crack the code" single-handedly within a reasonable timeframe. For instance, Distributed Computing Technologies (distributed.net), with cooperation with Electronic Frontier Foundation (EFF), won RSA Security's "DES Challenge III" competition using a purpose built DES cracking supercomputer "Deep Crack", and a network of over 100,000 personal computers connected over the internet using distributed.net's client application [distributed.net 1999, RSA-Laboratories 1999].

2.5.4.2 Public Key Cryptography, Digital Certificates and PKI Systems

The issues in E-Commerce of authenticating users and to ensuring non-repudiation of transactions can be solved, in theory, by the use of Public Key Cryptography in the form of digital certificates. Systems that manage the issuing and revocation of digital certificates are called PKI (Public Key Infrastructure) Systems.

Public Key Cryptography, in essence, is a form of encryption where different keys were used for encryption and decryption. The keys used in Public Key Cryptography consist of a public key and a private key. While the private keys are kept private by their owners, public keys are published in public directories and stored as digital certificates, which are "signed" by a Certificate Authority (CA) to ensure their authenticity. When someone encrypts a document with the public key, only the person with corresponding private key can decrypt the encrypted document. Encrypting a document with a person's private key is referred to as "signing the document", for encryption with a private key is the only feasible way to produce a document that can be decrypted by a public key.

There are several ways to obtain signed digital certificates. For instance, in order for Bob to obtain a digital certificate signed by a Certificate Authority, the person will need to first generate a public/private key pair, and then he sends the public key, in the form of digital certificate, to the Certificate Authority for signing. The Certificate Authority will need to *positively identify* Bob before signing his digital certificate with their private key. The signed digital certificate can then be used by Bob to authenticate with other systems or users.

The certificate authority, by positively identifying Bob, infers that Bob, not some other person, is the applicant of that particular digital certificate. The positive identification process is important for the issuing of digital certificates by the certificate authority as firstly issuing certificates to persons with shady identities may have serious consequences (imagine a fraudster claiming to be your local bank manager sending you a signed message requesting your account information, or a foreign spy posing as the Prime Minister sending a signed message to the Intelligence Agency requesting classified intelligence information). Secondly it is of the certificate authority's interest to verify the identities of their applicants as given their position as the Trusted Third Party, they are the primary source of identity information when a user enquires about Bob's digital certificate.

The there are currently two approaches in positively identifying the applicant. The first approach, used by many Certificate Authorities, is to arrange an interview with the certificate applicant in person, which may involve the applicant visiting the Certificate Authority's office. The second approach, which is currently used by Thawte [Thawte 2004], is to associate with the certificates "trust points", and delegate certain holders of their digital certificates as "Notaries", who can award "trust points" to other certificate holders. When the certificate applicant initially obtains a digital certificate from Thawte, he has no trust points and his name is not on the certificate itself. He then has to visit the notaries in order to obtain trust points. A notary may award a limited number of trust points to each certificate holder. A Thawte certificate holder may put his name onto his digital certificate once he has accumulated 50 trust points. A Thawte certificate holder may become a notary himself once he has obtained 100 trust points.

The usage model for digital certificates is illustrated in Figure 2-3, and can be explained in the following scenario: when Alice receives a document signed by Bob (i.e. encrypted using Bob's private key), she first fetches Bob's digital certificate from a certificate repository, she then retrieves a list of revoked certificates called the Certificate Revocation List (CRL) from the same or another repository, and checks Bob's certificate against the CRL. Once Alice verifies that Bob's certificate is still valid she may proceed with decrypting Bob's document with the public key stored in Bob's certificate.

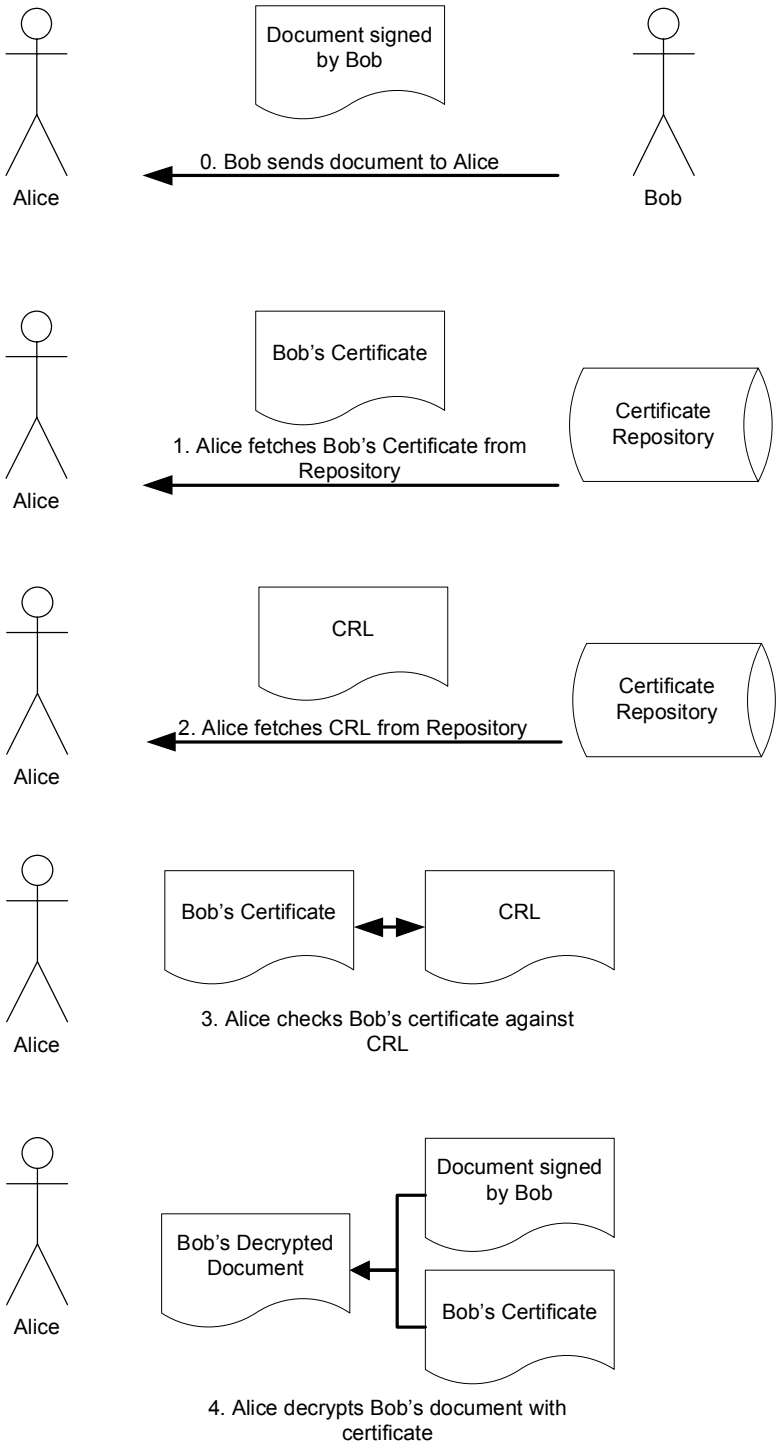


Figure 2-3 X.509 Certificate Usage Model (adapted from [Gutmann 2002])

We note that there is a race condition between Alice's retrieval of the CRL in step 2 and her subsequent actions in steps 3 and 4, as Bob's certificate may be declared invalid after Alice has retrieved the CRL from the certificate authority. The problems with CRLs are to be discussed later in this section.

Despite the security offered by Public Key Cryptography, there are shortcomings in the implementation and usage of digital certificates. A lot of technical issues with PKI systems are presented by Peter Gutmann [Gutmann 2002], and a brief summary of his research will be presented here.

There are two main areas of technical concern with regard to the design and implementation of PKI systems: the certificate directory, and the revocation mechanism.

Technical concerns with regard to certificate directories can be summarised as the "Which directory?" problem and the "Which John Smith?" problem [Gutmann 2002]. Both the "Which directory?" and the "Which John Smith?" problem are somewhat related to the X.500 directory standard, and it is explained below.

Initially when the use of digital certificates was being incorporated into the X.500 directory standard its proponents proposed a hieratical structure for the certificate directory, where a path through the directory is characterised by a distinguish name (DN), which comprises of a series of relative distinguish names (RDN). At the end of the path is an entry which contains the actual data, and in the context of certificate directories, it will be the user's digital certificate. Such a directory model is illustrated in Figure 2-4.

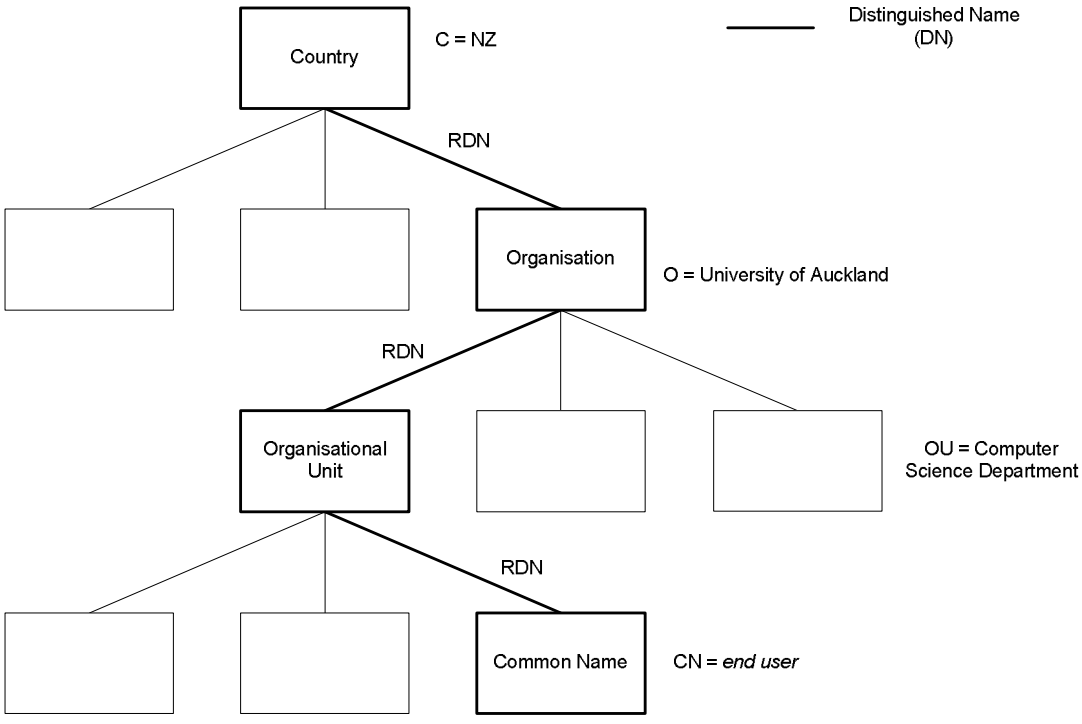


Figure 2-4 X.500 directory model (adapted from [Gutmann 2002])

The owner of a digital certificate may provide information that allows other people to uniquely identify himself. While such information may be anything from his passport number to his postal address, in reality the actual information stored in the digital certificate can be as little as his email address and his generic location (for example, *Auckland, New Zealand*). While providing more information on the digital certificate will help in uniquely identifying the owner of the certificate, such additional information may raise privacy concerns.

The "Which directory?" problem arises, using the scenario illustrated in Figure 2-3 as an example, when Alice tries to look for Bob's certificate in a certificate repository. Firstly Alice has no clear idea where to fetch Bob's digital certificate from upon receipt of his signed document, since there are numerous certificate repositories as opposed to a single, global distributed certificate repository. Secondly, even if Alice finds the correct repository, there is no way for Alice to determine which DN should be used in finding Bob's certificate. Thirdly even if Alice already has Bob's certificate she still has no clear idea where to fetch the CRL from, as the revocation entry for Bob's certificate may reside in a repository different to where Bob's certificate is located.

The "Which John Smith?" problem is concerned with the problem of the association of digital certificates to their owners and the fact that there might be more than one person with the same name in the directory, making the task of finding the right person and the right certificate even more difficult. Using the scenario illustrated in Figure 2-3, even if Alice happens to look in the right repository, she might encounter more than one certificate with the owner Bob written on the certificate. There was a case where there were people with the same first, middle and last name in the same Organisation Unit (OU) within the certificate directory [Gutmann 2002].

Attempts are made to overcome the naming problem within the certificate directory in the original implementation of digital certificates, they include the SPKI standard, PGP, and the X.509v3 standard.

Another concern with regard to the design and implementation of PKI systems is the problems associated with revocation. Traditionally in the X.509 directory standard the revocation of certificates is managed by Certificate Revocation Lists, which are based on credit-card blacklists used in the 1970's [Gutmann 2002]. However this method of using revocation lists for managing of revoked certificates

suffers the same problems as its credit card counterparts: they are not issued frequently enough to prevent misuse of compromised certificates; checking of certificates against the CRL is time-consuming; distribution of revocation lists is costly in terms of bandwidth requirements (the size of the CRL grows as the number of revoked certificates increases, and each web client has to download the same CRL just to check the revocation status of the certificates they receive); and the distribution of the CRL can be interrupted by conducting a denial-of-service attack on the distribution server. Subsequently the Online Certificate Status Protocol (OCSP) has been proposed to overcome the problem associated with certificate revocation [Gutmann 2002].

While proponents of digital certificates may argue that you can associate a digital certificate to an entity in the real world, with the quality of information currently stored in digital certificates it is more appropriate to say that you can associate a digital certificate to an electronic pseudonym, and that pseudonym to a particular entity in the real world. The association of electronic pseudonyms to real world entities can be of a weak nature, this is illustrated firstly by the fact that people often have multiple email accounts, secondly by the fact that family members often share a single email account, and thirdly nicknames in IRC (Internet Relay Chat) and instant messaging systems can be changed on the fly. Thus it is inherent that the association of digital certificates to real world entities can also be of a weak nature, hence weakening the non-repudiation property of digital certificates that some proponents base their marketing on.

With the present implementation of digital certificates we rely solely on the certificate authority's identity verification process for the positive identification of the certificate applicant, and we have little or no access to the verification data collected and used by the certificate authority for our own assessments of the identity of a certificate's owner. The weakness in association of digital certificates to real-world entities exposes two problems with the identity verification process. Firstly the certificate authority might misidentify a pseudonym to a real-world entity when issuing or certifying certificates, secondly someone reading a digital certificate might misidentify the pseudonym named on the certificate to a real-world entity involved in some transaction based on this certificate.

2.5.5 Payment Intermediaries or Escrow Agents

Payment Intermediaries and Escrow Agents are trusted third parties that handle the transfer of funds or goods between the parties in a transaction. The main difference between Payment Intermediaries and Escrow Agents is that Escrow Agents handle the transfer of both funds and goods, whereas Payment Intermediaries only handle the transfer of funds [Sorkin 2001]. Payment intermediaries and Escrow Agents protect users from exposing sensitive personal information such as credit card numbers and postal addresses to other people online. PayPal [PayPal 2004] is an example of a Payment Intermediary – they provide a service where by users can send and receive payments online with the counterpart's email address as their only information.

With Escrow Agents, the parties in a transaction initially send their payment and goods to the Escrow Agent elected by the transacting parties. Once the transaction parties verify that payment and the goods meet the terms of the transaction the Escrow Agent delivers the goods and payment to the respective parties. This prevents the possibility of fraud where the seller of a transaction receives the payment but never delivers the goods or the buyer receives the goods but never pays the seller for it.

Transactions using online escrow services such as Escrow.com are completed as follows: Initially the buyer and the seller sign up for an account at an agreed escrow service provider and agree on the terms of the transaction; the buyer pays the escrow service provider for the goods, and the payment is held in a trust account; the seller is then instructed to ship the goods using an approved courier service and to record the tracking number so the escrow service provider can enquire about the shipment status of the goods; the buyer receives and inspects the goods to make sure that it is what he purchased; and finally the escrow service provider pays the seller for the goods.

2.5.6 Alternate Dispute Resolution and the Legal System

The legal system has traditionally been the method consumers and businesses use to resolve their differences. One of the disputing parties file a complaint or a suit against the other party, and depending on the circumstances, the disputing parties may reach an out of court settlement, or the case will proceed to a trial and a decision will be made for the case.

With the emergence of the internet there are legal barriers to resolve differences involving online transactions. The borderless nature of the internet creates issues in utilising the legal system, such as which country or state's law applies to the dispute, and whether decisions made by the courts or tribunals are enforceable across borders of states and countries [Carblanc 2000].

Other concerns with regard to the utilisation of the legal system are the costs associated with court proceedings, which may exceed the value of the goods or services in dispute [Carblanc 2000], and the length of the legal proceedings, which may be too long for the value of the decision to be of any significant value [Carblanc 2000] or too slow to have an immediate impact for the disputing parties.

Alternative Dispute Resolution systems ("ADR") are mechanisms and procedures that are designed to resolve differences, both in offline and online environments. Unlike the legal system whereby the rules of procedure are imposed by the courts, for an ADR process such rules may be imposed by either the disputing parties or by the ADR provider; decisions reached via an ADR process can be binding or non-binding to one or more parties of the dispute, whereas it is legally binding to all disputing parties if the decision was reached via the legal system. ADR systems are often preferred over the legal system for informality, economic, and simplicity reasons.

The processes of resolving differences using ADR systems are as follows: initially a party of a transaction in dispute files a complaint to a third-party ADR provider, and the ADR provider notifies the other party or parties of the transaction of the complaint. Then a series of dialogues occur between the disputing parties and a neutral third-party as the mediator as they try to settle the dispute.

3 Our Qualitative Trust Model

Writing an interesting literature review is a difficult task, as we can only be so interesting before the realities of summarising all that not-so-interesting material begin to haunt us. Luckily in this chapter our readers will not see much summarisation of the reviewed literature, as most of the stuff in this chapter is our original material (our P.R.E.C.I.O.U.S.).

In this chapter we present the process that we undertook in developing our qualitative trust model. We first describe our initial considerations for the model, such as the model's objective and the inclusion of various dimensions of trust as described in our literature review. We then present the definitions we have chosen for our qualitative trust model, and the qualitative trust model itself.

3.1 Initial Considerations for Our Model

At the initial development stages of our trust model we compile a list of things that we need to consider, such as the objectives of the model, the requirements of the various components in the model, the inclusion or exclusion of concepts in our trust model, and the extent we include/exclude those concepts in our trust model.

We provide our initial considerations for our trust model in the following areas: the objective of the model, requirements for the definitions of terms used in the model, considerations for the social levels of trust, considerations for the quality of trust, and considerations for the quantity of trust.

3.1.1 Objective of Our Trust Model

The objective for our trust model is to enable us to analyze various online trading systems such as eBay and Amazon.com for mechanisms that handle or manage trust information for their users. From the identification of mechanisms in those trading systems by our trust model we should be able to draw conclusions as to whether those systems facilitate the development of trust relationships among the systems' users.

The model itself should be simple to apply to the analysis of various online trading systems. Thus we apply the "Occam's razor" principle during our model building process – the simplest model is preferred until it is proved to be inadequate.

3.1.2 Definition Requirements

In the previous chapter we mentioned the problems associated with modelling and applying trust in computer systems is often to do with various subjective, intuitive definitions that are made for trust by individuals. Gollmann suggests that a person attempting to understand a trust system should "wipe the slate clean" (i.e. to throw away the bias to their own intuitive definitions of trust) and understand the working the trust system from the creator's point of view [Gollmann 2002]. We develop a set of criteria in deriving our working definitions for our model, and they are as follows.

1. The definitions for the terms that are used in our model must reify the abstract concepts that the terms represent, to the point where someone can take our working definitions and design a system from them.
2. The definitions must be applicable to a broad range of situations such as online trading, dating services, and product review services.

We acknowledge the conflict that is inherent in satisfying both criteria, as it can be observed that something that can be reified may not be broad enough to be applicable to various situations. Therefore we will let criterion (1) take precedence over criterion (2) where conflict arises.

3.1.3 Social Levels of Trust

We observed that various levels of trust are involved when interacting with a computer system. For example, when conducting transactions in eBay we trust eBay as an organisation that they will process transactions correctly; we also trust other traders at eBay that they will act legitimately and not to defraud us or mislead us by feeding false information or withholding information; we might also place trust in ourselves not to waste too much money or time at eBay.

We recognise that building a model that takes into account every aspect from all social levels of trust will unnecessarily complicate the model (as discussed in section 2.4.4 about Marsh's trust model). Therefore there is a need for us to apply the Occam's razor principle and put a limit to the level of detail that the model will cover for each social level of trust.

From the literature that we surveyed it is observed that there is a level of subjectiveness which influences the trusting choice an individual makes [Rempel

1985, Deutch 1973], however we argue that in an online trading environment the workings among personality variables becomes less relevant as the focus is shifted from the inner workings that results in a person's general trusting attitude (disposition) to the process that a person undertakes in placing his trust in other individuals. Luhmann asserted that "… very different personality systems can be functionally equivalent in social systems…" [Luhmann 1979, Page 9, note 10]. We therefore will not incorporate an individual's disposition in our trust model, and we will not model the personality system itself.

Some of the literature on Interpersonal Trust that asserts that past experiences and previous behaviours are important factor for the development of trust among individuals [Rempel 1985, Mui 2002]. Several trust models rely on this assertion, using past behaviours as a basis for determining the trustworthiness of an individual [Abdul-Rahman 2000, Aberer 2001, Mui 2002]. Accordingly, we include in our trust model the trusted party's previous interaction with the trusting party as a direct input to the trusting party's decision to trust the trusted party.

Some of the literature on E-Commerce trust focusses on Organisational Trust, that is, the development of trust relationship between an individual and an organisation (made up of a group of individuals) [Cheskin 1999, Fung 1999]. Barber and Luhmann also described aspects of Organisational Trust in their monographs [Barber 1983, Luhmann 1979]. Accordingly, in our model an organisation can be either a trusting or a trusted party, or both.

Many E-Commerce "trust management" or trading systems, both proposed and currently available, involve the utilisation of Trusted Third Parties [Atif 2002, Daignault 2002, eBay 2003a, Horne 2001]. These Trusted Third Parties are often organisations. In our model, we identify the users' trust in the Trusted Third Party as Institutional Trust, which is a form of Organisation Trust. Accordingly, we include the Trusted Third Party as an actor in our model, either as a "trust information provider" or as a "transaction completion intermediary".

3.1.4 Quality of Trust

The "quality of trust" is concerned with the messages that flow among the participants in a trust development mechanism. Our trust model must capture the message flows that occur inside a trading system, thus enabling the analysis the trading system for mechanisms that facilitates trust development.

In section 2.3.2 of our literature review we briefly described two qualitative trust models proposed by Jøsang and Mui et al [Jøsang 1997, Mui 2002]. Jøsang's qualitative concerns with the distinction between passionate and rational entities and interactions among those entities in a relatively abstract level (that is, without reference to any specific type of action or communication). We find Jøsang's trust model inadequate for our objective as the model itself focuses only on static one-off classification of entities in an online trading system, and does not focus or enable the dynamic development of trust during E-Commerce transactions.

Mui et al's [Mui 2002] qualitative trust model is concerned with the influences among Reciprocity, Reputation and Trust. They assert the following three influences among Reciprocity, Reputation and Trust. Firstly the outcome of reciprocity influences the reputation of the participants. Secondly the reputation a participant has influences how the other people's trust in them. And lastly other people's trust in a participant influences the possibility of reciprocities in the future. The influences among the three components of Mui et al's qualitative trust model are illustrated in Figure 3-1. We find Mui et al's trust model adequate for the development of our trust model, as the model itself has an adequate level of detail, and that it focuses on the dynamic development of trust during E-Commerce transactions, as opposed to a static one-off evaluation of trust at one point in an E-Commerce scenario.

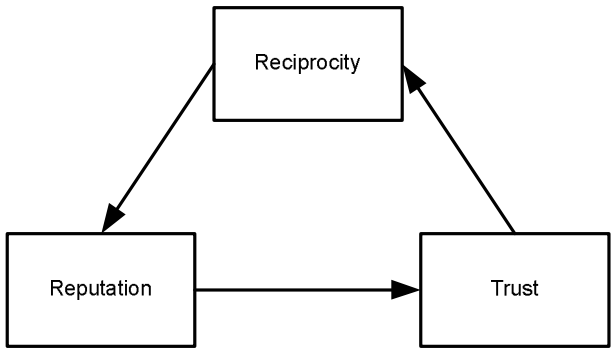


Figure 3-1 Diagram illustrating the relationships among Trust, Reputation and Reciprocity in Mui et al's trust model [Mui 2002]. The direction of the arrows indicates the direction of influence among the variables.

We have found (see Section 2.3.2 and above) that Mui et al's qualitative trust model can be applied to a variety of online trading systems currently available. For example, in eBay the outcomes of trader X's auction will affect his reputation once the counter-party posts a feedback and rating about trader X (i.e. reciprocity

influencing reputation). Trader's overall rating at eBay, when obtained by other users, will affect how the other users trust trader X as a reliable trader (i.e. reputation influencing trust). The level of trust the other users place in trader X might encourage those users to participate in future auctions run by trader X (i.e. trust influencing reciprocity). The close relationship among trust, reputation and reciprocity indicates that examining the reciprocity and reputation aspects of online trading systems will improve the quality of our analysis of those systems for trust development properties. Accordingly we have examined the definitions for reciprocity and reputation for our trust model.

While the general interactions in Mui et al's trust model are a good starting point for our own analysis-oriented trust model, we find that their definitions for the fundamental terms are too narrow to satisfy our definition criteria (see section 3.2.1 for our discussion of their definitions, and Section 3.1.2 for our criteria). Thus we have adopted Mui et al's qualitative trust model as a foundation for our trust model, but we have redefined their fundamental terms.

3.1.5 Quantity of Trust

The "quantity of trust" indicates how much trust one entity has in another. In Section 2.4, we explored both theoretical [Rempel 1985, Fung 1999, Cheskin 1999] and mathematical models [Abdul-Rahman 1997, Abdul-Rahman 2000, Aberer 2001, March 1994, Mui 2002] which approximate or calculate the amount of trust in a trust relationship.

We believe that calculating the amount of trust will unnecessarily complicate the model and will not improve our analysis of online trading systems. Therefore we have not included such quantitative metrics in our trust model.

3.2 Developing Our Trust Model

In this section we first present our discussion on the existing definitions of the terms *trust*, *reputation* and *reciprocity*. We then present our definitions for those terms which are used in our trust model. Lastly we present our models: a generic Entity-Interaction model and a generic Trust model.

3.2.1 Discussions on Existing Definitions

In this section definitions of the terms *trust*, *reputation* and *reciprocity* from various sources are compared and discussed. Such sources include the Oxford English

Dictionary [Oxford 2003], Gambetta [Gambetta 1988b] in his research in trust, Abdul-Rahman and Hailes [Abdul-Rahman 2000] and Mui et al [Mui 2002] in their research of quantitative trust models. Definitions of the terms from the Oxford English Dictionary can be referred to in section 2.1, while other definitions are mentioned before its discussion if they have not been mentioned before.

3.2.1.1 Discussion on Existing Definitions of Trust

There are two other major definitions of the term *trust* beside the dictionary definitions mentioned in section 2.1: Diego Gambetta's definition and Mui et al's definition:

> Trust (or symmetrically, distrust) is a particular level of subjective probability with which an agent assess that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action.
>
> [Gambetta 1988a]

> Trust [is] a subjective expectation an agent has about another's future behaviour based on the history of their encounters.
>
> [Mui 2002]

Abdul-Rahman and Hailes' definition of the term *trust* in their work on quantitative trust models [Abdul-Rahman 2000] is a slight modification of Gambetta's original definition of trust. However we note that they put particular emphasis to the fact that they only taking the term "subjective probability" as an indication that there exists different levels of trust, rather than as a mathematical concept.

Bernard Barber [Barber 1983] and Niklas Luhmann [Luhmann 1979] described trust as some form of expectation, and Morton Deutch [Deutch 1973] described trust as some form of confidence. However none of the three authors provided a precise definition for the term *trust* itself, therefore we can only discuss their concepts with relation to the definitions mentioned earlier.

The definitions of the term *trust* provided by the Oxford English Dictionary [Oxford 2003] provides us with general ideas and initial insights, such as the fact that trust is something to do with confidence, expectation and reliability, and its does not involve deep investigation or strong evidence.

However its definitions are either too vague or too specialised to be used "as is" in our model, which is tailored for the analysis of online trading systems. For example, the "something" in definition 2 of the term *trust* in section 2.1 is ambiguous and needs to be elaborated further, and definition 4b of the term *trust* is too specialised as it imbues the term with a sense of obligation and responsibility which may apply in the legal profession (as described in Barber's three expectations of trust [Barber 1983]), but may not apply in online trading systems (for example, users in the Kazaa file sharing network are not obliged to share files, nor it is their responsibility to share only good quality files).

Gambetta's definition of the term *trust* also provides us with ideas as to the concept. Firstly *trust* and *distrust* are qualitative opposites (as Luhmann asserted in his monograph [Luhmann 1979]). Secondly there exist different levels of trust. Thirdly the term "subjective probability" implies that trust varies from one person to another. Fourthly similar to the Oxford English Dictionary's definition trust involves little investigation or evidence. And lastly trust is a context sensitive concept, for example we would trust the gardener to look after the plants in the garden but we might not trust him the same way to look after our kids.

The use of the term "probability" in Gambetta's definition of the term *trust* implies that trust is a transitive property [Abdul-Rahman 2000]. However, trust is not bi-directional nor is it transitive [Abdul-Rahman 2000, Jøsang 1997]. Just because Alice trusts Bob to some degree does not imply that Bob trust Alice to the same degree. If Alice trust Sally and Sally trusts Bob, it does not imply that Alice trusts Bob to the same degree that Sally trusts Bob.

Mui et al's definition of the term *trust* is narrowly defined to suit the purposes of their research – to derive a computational model for trust and reputation. This is evident in their work as they defined trust as a "summary quantity that an agent has toward another based on *a number of former encounters* between them" [Mui 2002]. The narrowness of their definition lies in the fact that they only consider the encounters between the trusting and trusted agents, and do not consider the encounters that the trusted agent has with other agents. Based on their definition of the term *trust* the trust value of a reputable agent X in another reputable agent Y would be zero if agent X and agent Y had no former encounters. In reality agent X could compute some sort of initial trust value for agent Y based on the former encounters agent Y has with other agents in the system (that is, agent X will enquire from other agents about

agent Y's past behaviour). Thus we argue that the narrowness of Mui et al's definition of the term *trust* does not reify the abstract concepts that the term represents.

3.2.1.2 Discussion of Existing Definitions of Reputation

Besides the definitions provided by the Oxford English Dictionary [Oxford 2003] in section 2.1, Abdul-Rahman and Hailes and Mui et al have provided their own definitions for the term *reputation*:

> A reputation is an expectation about an agent's behaviour based on information about or observation of its past behaviour.
>
> [Abdul-Rahman 2000]

> Reputation [is a] perception that an agent creates through past actions about its intentions and norms.
>
> [Mui 2002]

The definitions provided by the Oxford English Dictionary [Oxford 2003] for the term *reputation* allow us to gain an initial insight into the abstract concepts behind the term itself. For example reputation is a perception or estimate about someone or something's characteristics. However, the dictionary definitions fail to mention any correlations between reputation and past behaviour, which is included in definitions from Abdul-Rahman and Hailes' and Mui et al's research.

At first glance Abdul-Rahman and Hailes' definition for the term *reputation* appears to be very similar, if not identical, to Mui et al's definition for trust. This is possibly due to the fact that they use a modified version of Gambetta's definition for their definition of trust. However, treating reputation as expectations clearly confuses with trust as a notion of expectation (as described by Barber and Luhmann [Barber 1983, Luhmann 1979]).

Mui et al's definition for reputation as a perception complements the dictionary definitions. However their definition is again too narrow to be applicable over a broad range of trading systems. Firstly the wording of the definition itself fails to take into account the observations or opinions made by others about the agent with the reputation (e.g. the trusted agent), even though they include those observations and opinions as part of the definition in their subsequent discussion [Mui 2002]. Secondly their definition implies that the agent with the reputation has control over the perception (as he "creates" the perception in the first place), in reality the only

thing he can control is his *behaviour*. The control on a perception resides on the one who *perceives*, rather than the one who is *being perceived*.

3.2.1.3 Discussion of Existing Definitions of Reciprocity

Besides the Oxford English Dictionary [Oxford 2003] the only other definition for the term reciprocity is provided by Mui et al:

> Reciprocity [is a] mutual exchange of deeds (such as favour or revenge)
>
> [Mui 2002]

The definitions of the term reciprocity provided by the Oxford English Dictionary [Oxford 2003] and Mui et al [Mui 2002] are strikingly similar – they both refer to a mutual exchange of some sort. While the dictionary definition states that reciprocity concerns the exchange between *two* parties, Mui et al points out that there are two types of reciprocity: *direct* reciprocity where the exchange of deeds is between only the two agents of concern, and *indirect* reciprocity where the exchange of deeds between the two agents is mediated by a third agent in between [Mui 2002].

3.2.2 Deriving our own Working Definitions

Our definitions must adhere to the criteria stated in section 3.1.1. To avoid ambiguities arising from the English language we use the plural form (i.e. we) for the subject of the definition and the singular form (i.e. he/she/it) for the object of the definition (i.e. "the other person").

3.2.2.1 Working definition for Trust

We derive our working definition for the term trust from both Gambetta's [Gambetta 1988a] and Mui et al's [Mui 2002] definitions:

> *Trust is a particular level of subjective expectation we have on an agent's future behaviour, both before we can monitor such behaviour (or independently of our capacity of ever to be able to monitor it), and in a context in which it affects our own action.*

We replace the phrase "subjective probability" in Gambetta's definition with "subjective expectation" in Mui et al's to firstly remove the possible perception that

trust is just some mathematical number, and secondly to reiterate our view of trust as an expectation in online trading systems.

3.2.2.2 Working definition for Reputation

We derive our working definition for reputation from both Abdul-Rahman and Hailes' [Abdul-Rahman 2000] and Mui et al's [Mui 2002] definitions:

Reputation is a general perception we have about an agent's intentions and norms based on information about or observations of its past behaviour.

We replace the phrase "expectation" in Abdul-Rahman's definition in favour of "general perception" in Mui et al's to firstly avoid confusions that may arise when viewing this definition along with our working definition for trust, and secondly to stress that reputation is a perception about something, as stated in Mui et al's and the dictionary definitions.

3.2.2.3 Working definition for Reciprocity

We use Mui et al's definition of reciprocity [Mui 2002] for our working definition of reciprocity:

Reciprocity is a mutual exchange of deeds (such as favour or revenge).

Mui et al's definition was chosen over Oxford English Dictionary's definition for the conciseness of its wording.

3.2.2.4 Working definition for Online Trading System

To avoid ambiguities with intuitive definitions (as observed by McKnight [McKnight 2001]) we formally define the term "Online Trading System" as follows:

An Online Trading System is a system of computing devices (consist of hardware and software) such that it enables the exchange of goods and services among the users using the system, and operates in a networked environment (such as the Internet or local electronic bulletin boards).

We note that our definition does not limit the operating environment to only the Internet. For example, the New Zealand Stock Exchange's (NZX hereafter) FASTER platform is a computer system that enables the trading and settlement of securities among participating NZX firms and stockbrokers [NZX 2004a]. The participants of the FASTER platform either connect to the FASTER network via dedicated Frame Relay circuits or via the NZX VPN (Virtual Private Network) [NZX 2004b].

3.2.2.5 Distinctions between our working definitions of Trust and Reputation

We would like to point out some of the distinctions between trust and reputation that we have discovered during the process of deriving our working definitions of trust and reputation, and they are as follows:

- *Trust* concerns with expectations of future behaviour, whereas *reputation* concerns with perceptions based on past behaviour.
- *Trust* is a concept that is context-dependent, whereas *reputation* is a general concept that is context-independent.
- *Trust* is assessment on an individual level ("Should *I* trust him?"), whereas *reputation* is opinion on a community level ("The *others* say he is a reliable person.").

3.2.3 Definition of Miscellaneous Terms

We would like to take this opportunity to clarify and provide definitions for the terms in addition to *Trust*, *Reputation* and *Reciprocity* (discussed in section 3.2.2) that we have used both in our model and for the remainder of this thesis. We feel that this is necessary to firstly avoid conflicting intuitive definitions that this thesis's readers may have, and secondly to avoid confusions that may arise due to the ambiguities of the English language.

We define the term *entity* in our model as *something that exists as a particular and discrete unit* [Dictionary.com 2004]. We classify parties into two types of entities in our model:

- An *Actor* is an entity that is either a human or an organisation.
- An *Agent* is a non-human entity which handles/manipulates trust and reputation information or acts on behalf of an Actor.

Those agents may be (but are not necessarily) of an AI nature. Thus we use the terms *manipulate* and *handle* to emphasise that the agents do not "reason" about the trust and reputation information given. We assume that an actor has complete control over its agent (that is, we ignore situations of "agent theft" and unintended agent behaviour).

We introduce the following actors and terms that we use both in our model and in our analysis. Given a phrase "Alice trusts Bob because she believed a report on Bob's reputation produced by Sally or Sally's computer system Sigma", we define the following actors:

- Actor *Alice* is the *trusting party*.
- Actor *Bob* is the *trusted party*.
- Actor *Sally* is the *trusted third party*, that is, a party already deemed trustworthy by both Alice and Bob.

In situations where agents are involved in handling/manipulating trust and reputation information or acting on behalf of any of the actors defined above, we use the following terms to distinguish the various agents:

- *Alpha* is the agent handling/manipulating trust and reputation information or acting on behalf of actor Alice.
- *Beta* is the agent handling/manipulating trust and reputation information or acting on behalf of actor Bob.
- *Sigma* is the agent handling/manipulating trust and reputation information or acting on behalf of actor Sally.

In situations where an actor has control over more than one agent, we subscript each of the agent's names with a number. For example, if actor Sally has two agents acting on her behalf, we name her two agents $Sigma_1$ and $Sigma_2$ respectively. We assert that an agent can only have one actor as its owner.

3.2.4 Our Generic Entity-Interaction Model

The Entity-Interaction Model is formulated by the author in his previous research [Lai 2002] (It was called the *Party-Agent model* in his previous research) as a tool to preliminary analysis of the system in terms of its general architecture and any notable characteristics. In this model the primary concern is the identification of entities and interactions *external* to the entities. Interactions *internal* to an entity are allowed but are not modelled in the Entity-Interaction Model.

The Entity-Interaction model is structured as illustrated in Figure 3-2: an actor may have control over an arbitrary number of agents, but an agent can only be controlled by one actor.

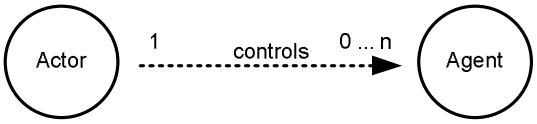


Figure 3-2 An illustration of the relationship between an Actor and an Agent. An actor may control any number of agents, but an agent can only be controlled by one actor.

If an actor has control over an agent, any interactions between the actor himself to other actors or agents not controlled by the actor will be conducted through his agent. The actor may interact directly with his or her agents. An actor may not interact directly with another actor's agent if the actor himself has agents acting on his behalf. Interactions internal to an actor or agent are not illustrated. As illustrated in Figure 3-3, $Actor_1$ cannot interact directly to $Actor_2$ as both actors have agents acting on their behalf ($Agent_1$ and $Agent_2$ respectively). $Actor_1$ cannot interact directly with $Agent_2$ as he/she has $Agent_1$ acting on his/her behalf. $Actor_2$ may interact directly with $Agent_2$, which he/she has ownership over. The interaction internal to $Actor_1$ should be excluded from Figure 3-3.

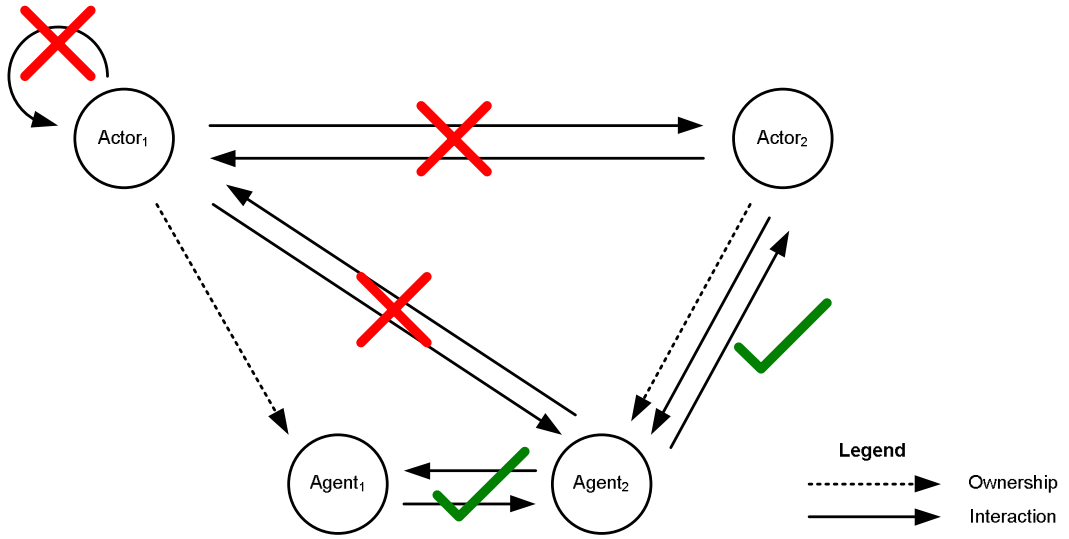


Figure 3-3 An illustration of the correct and incorrect message flows between actors when both actors have agents acting on their behalf.

If an actor does not have an agent acting on his or her behalf, the actor himself/herself will handle all interactions to him/her himself/herself. Again the actor without an agent cannot interact directly to another actor if the actor receiving the communication has an agent acting on his/her behalf. As illustrated in Figure 3-4, $Actor_1$ may interact directly with $Actor_2$ as both actors do not have agents acting on their behalf. However $Actor_2$ cannot interact directly with $Actor_3$ as $Actor_3$ has $Agent_3$ acting on his/her behalf. The interaction between $Actor_1$ and $Agent_3$ is correct.

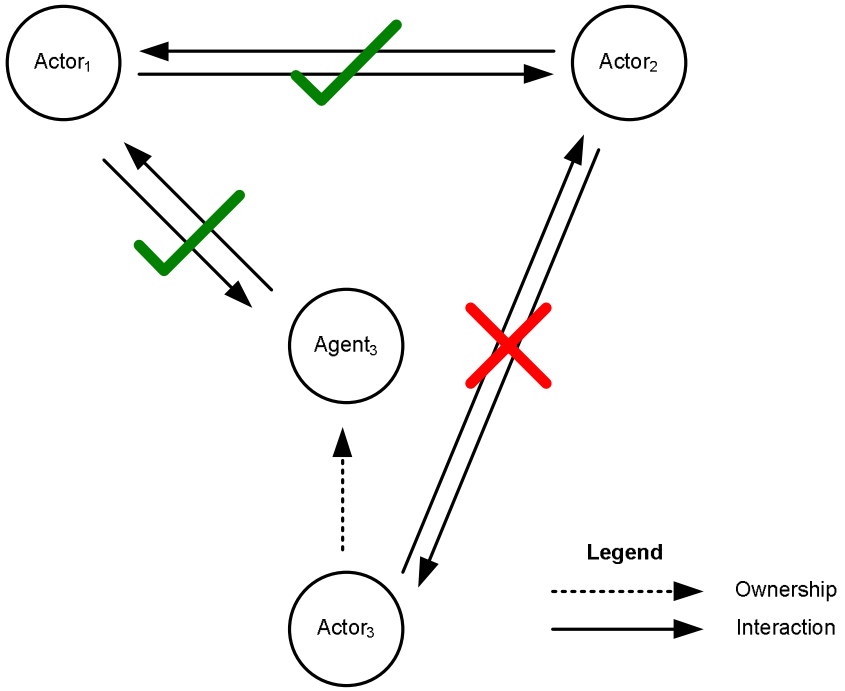


Figure 3-4 An illustration of the correct and incorrect message flows between actors and agents when some actors do not have agents acting on their behalf.

If an actor or an agent is interacting with a group of actors/agents of an arbitrary size, we indicate the group of actors/agents by a dotted rectangle around the repeating entities. As illustrated in Figure 3-5, $Actor_1$ is interacting in a similar way to a group of $Agent_2$'s, hence we encompass the $Actor_2$'s and $Agent_2$'s with a dotted rectangle.

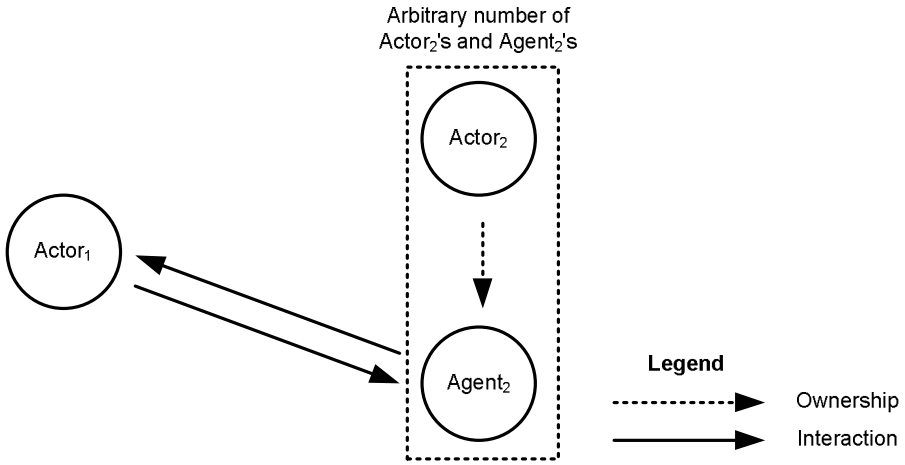


Figure 3-5 An illustration of the correct message flow when an actor is interacting with a group of actors/agent of arbitrary size.

Figure 3-6 illustrates an instance of the Entity-Interaction model that involves Alice, Bob, Sally and their respective agents. We note that an actor's agents may interact with each other, as illustrated by the interaction between Sally's agents $Sigma_1$ and $Sigma_2$. We also note that all arcs in our illustrations are unidirectional.

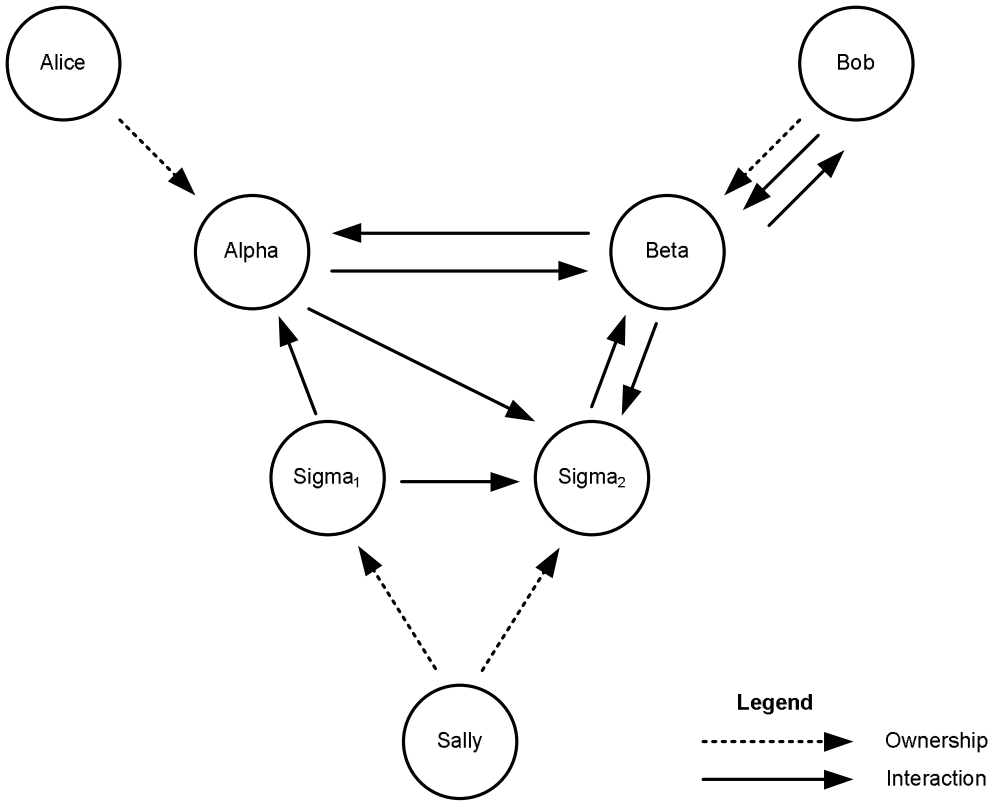


Figure 3-6 An instance of the Entity-Interaction model, showing the ownership of Alice's, Bob's and Sally's agents and the interactions among their respective agents.

3.2.5 Our Generic Trust Model

Our generic trust model is an extension to Mui et al's [Mui 2002] trust model. The model is developed to enable the analysis of trust, reputation and reciprocity properties of online trading systems.

We take a process-oriented approach in developing our generic trust model with three key types of components: *processes*, *messages* and *data-stores*:

- Process components take information from input messages and data-stores as inputs, and either produce messages as outputs, or update information in the data-stores.

- Messages are created and consumed by process components, and they are passed from one process component to another. Each message can only be consumed once.
- Data-store components are storage spaces for information that are used by process components. If a piece of information from a message is going to be used more than once, that piece of information is kept in a data-store. Data-stores can range from electronic databases, records on paper to a piece of memory in the human mind.

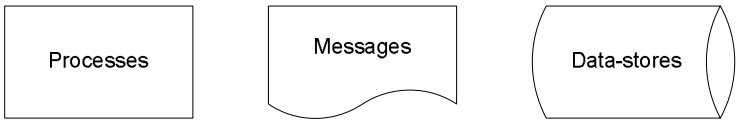


Figure 3-7 Diagram illustrating the representation of the three key components in our generic trust model

The process, message and data-store components in our generic trust model are represented as illustrated in Figure 3-7. Processes are represented as rectangles with the description of the specific process inside. Messages are represented as "documents" with the description of the contents of the messages inside. Data-stores are represented as cylinders on their sides, with the description of the information stored in the data-stores inside the cylinders.

We take on a closed system approach with modelling the interactions among these key components (that is, there are no external inputs or outputs in our generic trust model).

3.2.5.1 Key Components of our Generic Trust Model

Mui et al's qualitative trust model composed of *trust*, *reputation* and *reciprocity* and the influences among the three components reflects the reality of current online trading systems [Mui 2001]. We have expanded those three key components into six process components by distinguishing one actor's three process components from another actor's. The seven generic process components in our generic trust model are as follows:

- Alice's Trust

- Alice's Reputation
- Alice's Reciprocity
- Bob's Trust
- Bob's Reputation
- Bob's Reciprocity
- Sally's Reciprocity

By having those seven process components in our generic trust model we are able to clearly explain whose trust is influencing whose reciprocity, whose reciprocity is influencing whose reputation, and whose reputation is influencing whose trust. We model those influences as interactions among the process components in the form of messages.

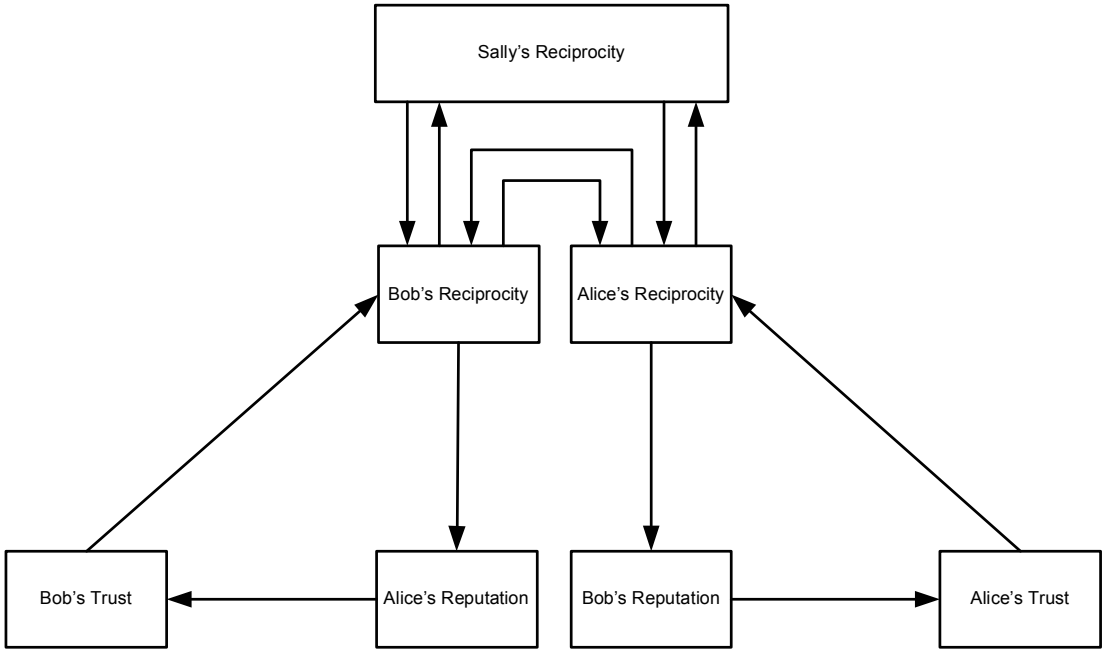


Figure 3-8 Diagram illustrating the overview of our generic trust model. The directions of the arrows indicate the direction of influence among the components.

The overview diagram of our generic trust model is illustrated in Figure 3-8. We would like to take this opportunity to explain some of our modelling rationale that is reflected in that diagram:

- We model Alice's Reciprocity as the influence to Bob's Reputation, as Alice's evaluation of the reciprocity will affect not Alice's reputation but Bob's, as he is the counterparty of the reciprocity.
- We model Bob's Reputation as the influence to Alice's Trust, as Bob's reputation is a factor that Alice may take into account when deciding whether she will trust Bob or otherwise.
- We model Alice's Trust as the influence to Alice's Reciprocity, as trust decision that Alice has made in the Alice's Trust process component will lead to Alice reciprocating with Bob (or Alice stopping the reciprocation from continuing).
- We also model Bob's side of the trust/reputation/reciprocity cycle because in an online trading system, Bob may or may not care about Alice's trustworthiness. The model needs to be able to cover both situations where Bob does not care about Alice's trustworthiness, and situations where Bob does have concerns about Alice's trustworthiness and wants to enquire about Alice's reputation and make his trust decision based on information about her reputation.
- We model the interactions between Alice's Reciprocity and Bob's Reciprocity process components as messages that flow between Alice and Bob. Those messages can either be communication messages (such as negotiation messages for terms of transaction), or actual exchange of goods and services.
- We model the interactions between Sally's Reciprocity and Alice's / Bob's Reciprocity process components as messages that flow between Sally and Alice / Bob.

We also identify the following key data-store components in our generic trust model which we find important in the storage and retrieval of information that are used by various process components. The key data-store components in our generic trust model are as follows:

- Alice's Memory of 1st Hand Experiences with Bob
- Bob's Memory of 1st Hand Experiences with Alice

- Sally's Reputation Database
- Bob's Memory of Outstanding Offers
- Alice's Memory of Worthwhile Offers

The rationales behind the identification of the key data-store components mentioned above are as follows:

- The Alice's/Bob's memory of 1st hand experiences data-stores are used to store personal experiences in the reciprocity process components, and used by the trust process components to retrieve information for trust-decision making processes.
- Sally's reputation database data-store is used by the reputation process components to store reputation information contributed by the traders in an online trading system (Alice and Bob in our generic trust model). The information within the reputation database is used to prepare reputation reports by the reputation process components.
- The memory of outstanding offers data-store (Bob's in this case) is used by traders to keep track of his/her offers.
- The memory of worthwhile offers data-store (Alice's in this case) is used by "shoppers" to keep track of the offers that he/she has found to be worthwhile.

After determining the key components in our generic trust model, the next step is to identify the types of interactions that flow among the process components, which is discussed in the next section.

3.2.5.2 A Generic Protocol for Developing Trust

In order to illustrate the types of interactions that flow among the process components in our generic trust model, we construct and make use of the following "generic" hypothetical scenario that involves Alice, Bob and Sally within an online trading system:

1. Offer Creation and Shopping Phase

a. “Bob decides to trade.” Bob decides to engage in some trading activity within Sally’s online trading system.
b. “Bob makes an offer.” He creates an offer within Sally’s online trading system and makes that offer available to other users in the online trading system.
c. “Alice goes shopping.” Alice looks in Sally’s online trading system for possible online trading activities she can engage herself in. She sends a request to Sally’s online trading system for a list of available offers.
d. “Sally sends a list of offers.” Sally’s online trading system processes Alice’s request and sends her a list of available offers, with Bob’s offer being one of them.

2. Alice’s Trust Evaluation Phase
    a. “Alice sends a request for reputation report.” Alice happens to come across Bob’s offer when browsing the list of available offers. She evaluates his offer, and becomes interested in trading with Bob. However, Alice has little knowledge about Bob as to whether he is a reliable trader or otherwise, therefore she requests a reputation report on Bob from Sally.
    b. “Sally processes Alice’s query.” Sally (or her agent Sigma) processes Alice’s request for a reputation report on Bob, and submits her reputation report on Bob back to Alice.
    c. “Alice decides to trust Bob’s offer.” Alice studies Sally’s reputation report on Bob, and based on the information on the reputation report and her personal experiences with Bob she decides that Bob is a reliable trader and can be trusted.
    d. “Alice decides to reciprocate with Bob.” After deciding that Bob is trustworthy enough as a trader she decides to trade with Bob. Alice sends a notification accepting Bob’s offer, along with her goods and services for fulfilling her terms of the transaction.
3. Offer-Acceptance Processing and Bob’s Trust Evaluation Phase (only one of 3a or 3b occurs)

a. “Bob reciprocates with Alice.” If Bob does not care about Alice’s trustworthiness or he trusts Alice enough that he does not need to enquire about her reputation on receipt of Alice’s notification of accepting his offer then he provides his goods and services to Alice for fulfilling his terms of the transaction.
b. If for whatever reasons Bob feels the need to consider Alice’s reputation before proceeding with the transaction, the following steps occur:
    i. “Bob decides to enquire about Alice’s reputation.” He decides to enquire about Alice’s reputation in the online trading system and requests a reputation report on Alice from Sally.
    ii. “Sally processes Bob’s query.” Sally processes Bob’s request and sends her reputation report on Alice back to him.
    iii. “Bob decides to trust Alice.” Bob studies Sally’s reputation report on Alice and based on the information on the reputation report and his personal experiences with Alice he decides that Alice is a reliable trader and can be trusted.
    iv. “Bob decides to reciprocate with Alice.” After deciding that Alice is trustworthy enough for Bob he decides to continue reciprocating with Alice, and delivers to her his goods and services.

4. Post-Transaction Evaluation Phase (steps 4a and 4b may occur in any order)
    a. After receiving Bob’s goods and services, Alice evaluates the quality of Bob’s reciprocation with her.
        i. “Alice evaluates the quality of Bob’s reciprocation.” After Alice has evaluated Bob’s reciprocation with her, she files a report about Bob’s reciprocity to Sally.
        ii. “Sally updates her database.” Sally updates her database upon receipt of Alice’s report and sends a notification to Bob about Alice’s report

b. After receiving Alice's goods and services, Bob evaluates the quality of Alice's reciprocation with him.
    i. "Bob evaluates the quality of Alice's reciprocation." After Bob finishes evaluating Alice's reciprocation with him, he files a report about Alice's reciprocity to Sally.
    ii. "Sally updates her database." Sally updates her database upon receipt of Bob's report and sends a notification to Alice about Bob's Report.

5. New Evaluation Notification Phase (the steps may occur in any order)
    a. "Bob updates his experiences with Alice." After reading Alice's report on Bob's reciprocity, Bob updates his personal experiences with Alice.
    b. "Alice updates her experiences with Bob." After reading Bob's report on Alice's reciprocity, Alice updates her personal experiences with Bob.

3.2.5.3 Modelling of Message Flows in our Generic Procotol

From our generic hypothetical scenario in section 3.2.5.2 we identify the various components that are involved and model the interactions among each of the components. We have diagrammed in detail our modelling of the message flows that takes place in the hypothetical scenario in Figure 3-9 and from Figure 6-1 to Figure 6-8 in the Appendix. We also explain our modelling rationale in each of the steps diagrammed in each of the figures.

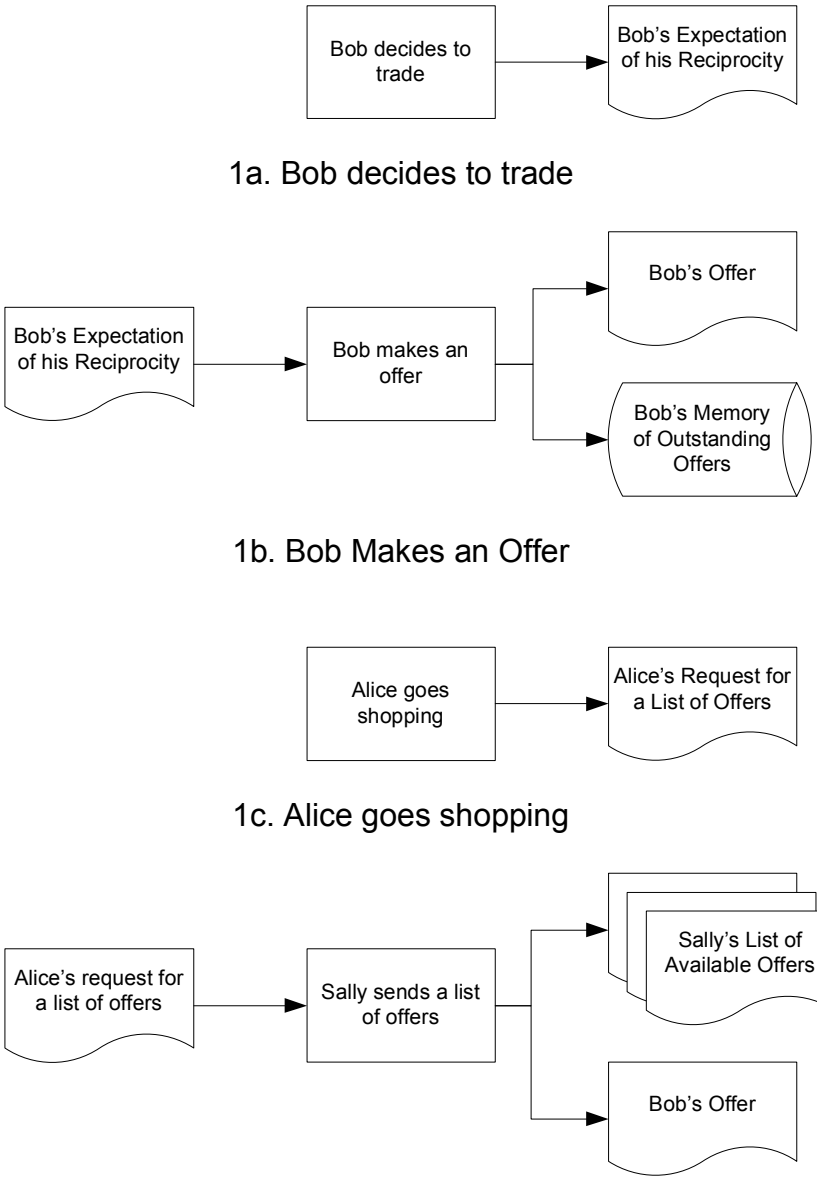


Figure 3-9 Diagram illustrating the interactions among various components in our generic trust model (steps 1a – 1d)

- In step 1a, "Bob decides to trade." (See our complete description of this step in our hypothetical scenario at page 51.) We envisage that after Bob makes his decision to reciprocate he will have some level of expectation about the outcome of his reciprocity in the online trading system. Thus we label this step's process component with Bob's decision to reciprocate, which results in an outgoing message conveying his expectation. *(See Table 3-1 for our summary analysis of this step: Bob sends an expectation message from his Trust component*

to his Reciprocity component. We categorise this step as falling in "Bob's Trust" in our illustrated in our overview diagram in Figure 3-8, and the expectation message as going from "Bob's Trust" to "Bob's Reciprocity".)

- In step 1b, "Bob makes an offer." We envisage that the actual offer-making happens as a result of his earlier decision to reciprocate in the online trading system, and that Bob keeps a record of his outstanding offers. Thus the offer-making process is a process component, taking the expectation message from step 1a as the input. We model the actual offer as an outgoing message component, and Bob's record of outstanding offers is a data-store component, which gets updated when Bob makes his offer available in the online trading system.
- In step 1c, "Alice goes shopping." We envisage that Alice's browsing involves sending a message to Sally's online trading system requesting a list of available offers. Thus the browsing process is a process component. Alice's browsing process produces a request for Sally's online trading system to produce a list of available offers, which we model as an outgoing message component.
- In step 1d, "Sally sends a list of offers." We envisage that in addition to Bob's Offer Sally's online trading system will send other offers for Alice to evaluate. Thus the process of sending offers is a process component, taking Alice's request for a list of offers message from step 1c as input. The sending process produces a list of available offers as a series of outgoing message components, along with it is Bob's Offer message (which we have emphasised by separating it from Sally's List of Available Offers message).

The remainder of the diagrams and the modelling rationales are provided and can be found in the Appendix in section 6.1.

After modelling the message flows in each of the steps into processes we categorise each of the processes into one of the six key process components discussed in section 3.2.5.1. Our complete categorisation of the process steps is illustrated in Table 3-1,Table 3-2 and Table 3-3.

Step	Description	Input Messages (Data-stores)	Output Messages (Data-stores)	Process Type
1a	Bob decides to trade		Bob's Expectation of his Reciprocity	Bob's Trust
1b	Bob makes an offer	Bob's Expectation of his Reciprocity	Bob's Offer (Bob's Memory of Outstanding Offers)	Bob's Reciprocity
1c	Alice goes shopping		Alice's Request for a List of Offers	Alice's Reciprocity
1d	Sally sends a list of offers	Alice's Request for a List of Offers	Sally's List of Available Offers Bob's Offer	Sally's Reciprocity
2a	Alice evaluates Bob's offer	Sally's List of Available Offers Bob's Offer	Alice's Query about Bob's Reputation (Alice Memory of Worthwhile Offers)	Alice's Reciprocity
2b	Sally's processes Alice's query	Alice's Query about Bob's Reputation (Sally's Reputation Database)	Reputation Report on Bob	Bob's Reputation
2c	Alice decides to trust Bob's offer	Reputation Report on Bob (Alice's Memory of 1st Hand Experiences with Bob)	Alice's Expectation of Bob's Trustworthiness	Alice's Trust
2d	Alice decides to reciprocate with Bob	Alice's Expectation of Bob's Trustworthiness (Alice Memory of Worthwhile Offers)	Alice's Notification of Acceptance to Bob Alice's Goods and Service to Bob (Alice's Memory of 1st Hand Experiences with Bob)	Alice's Reciprocity

Table 3-1 Table illustrating the categorisation of the process components and their input and output components in the hypothetical scenario (steps 1a – 2d)

Step	Description	Input Components (Data-stores)	Output Components (Data-stores)	Process Type
3a	Bob reciprocates with Alice	Alice's Notification of Acceptance to Bob (Bob's Memory of Outstanding offers)	Bob's Goods and Services to Alice (Bob's Memory of 1st Hand Experiences with Alice) (Bob's Memory of Outstanding offers)	Bob's Reciprocity
3b(i)	Bob decides to enquire about Alice's reputation	Alice's Notification of Acceptance to Bob (Bob's Memory of Outstanding offers)	Bob's Query about Alice's Reputation	Bob's Reciprocity
3b(ii)	Sally processes Bob's query	Bob's Query about Alice's Reputation (Sally's Reputation Database)	Reputation Report on Alice	Alice's Reputation
3b(iii)	Bob decides to trust Alice	Reputation Report on Alice (Bob's Memory of 1st Hand Experiences with Alice)	Bob's Expectation about Alice's Trustworthniness	Bob's Trust
3b(iv)	Bob decides to reciprocate with Alice	Bob's Expectation about Alice's Trustworthniness (Bob's Memory of Outstanding offers)	Bob's Goods and Services to Alice (Bob's Memory of 1st Hand Experiences with Alice) (Bob's Memory of Outstanding offers)	Bob's Reciprocity

Table 3-2 Table illustrating the categorisation of the process components and their input and output components in the hypothetical scenario (steps 3a - 3b(iv))

Step	Description	Input Components (Data-store)	Output Components (Data-store)	Process Type
4a(i)	Alice evaluates the quality of Bob's reciprocation	Bob's Goods and Services to Alice (Alice's Memory of 1st Hand Experiences with Bob)	Alice's Report to Sally about Bob's Reciprocation (Alice's Memory of 1st Hand Experiences with Bob)	Alice's Reciprocity
4a(ii)	Sally updates her database	Alice's Report to Sally about Bob's Reciprocation (Sally's Reputation Database)	Notification of Alice's Report on Bob's Reciprocity (Sally's Reputation Database)	Bob's Reputation
4b(i)	Bob evaluates the quality of Alice's reciprocation	Alice's Goods and Services to Bob (Bob's Memory of 1st Hand Experiences with Alice)	Bob's Report to Sally about Alice's Reciprocation (Bob's Memory of 1st Hand Experiences with Alice)	Bob's Reciprocity
4b(ii)	Sally updates her database	Bob's Report to Sally about Alice's Reciprocation (Sally's Reputation Database)	Notification of Bob's Report on Alice's Reciprocity (Sally's Reputation Database)	Alice's Reputation
5a	Bob updates his experiences with Alice	Notification of Alice's Report on Bob's Reciprocity (Bob's Memory of 1st Hand Experiences with Alice)	(Bob's Memory of 1st Hand Experiences with Alice)	Bob's Trust
5b	Alice updates her experiences with Bob	Notification of Bob's Report on Alice's Reciprocity (Alice's Memory of 1st Hand Experiences with Bob)	(Alice's Memory of 1st Hand Experiences with Bob)	Alice's Trust

Table 3-3 Table illustrating the categorisation of the process components and their input and output components in the hypothetical scenario (steps 4a(i) - 5b)

3.2.6 Summary and Discussion

We note that the flow of messages in these steps follow our model arcs; messages from Bob's Trust always go to Bob's Reciprocity, and never to any other process components. Also, our model accurately fits the sequencing of process steps: they circulate around the two triangular cycles of Figure 3-8, for example a message to Bob's Reciprocity triggers a message from Bob's Reciprocity to Alice's Reputation.

4 Applying our Trust Model on Real World Systems

We hope our readers are still holding on after reading all those countless bullet points, diagrams and tables in the previous chapter, for there are more to come in this chapter.

In this chapter we present our analysis of three online trading systems for trust development properties using both the generic Entity-Interaction model and the generic trust model described in Sections 3.2.4 and 3.2.5. We first describe the methodology we followed in conducting our analysis on each of the online trading systems, followed by our actual analysis of the three online trading systems.

4.1 Methodology for Analysis

The first step of our analysis is to construct a series of events that typically occur in the system in question. Each event consists of a decision, an action or both. The events are grouped by the stage of the scenario in which they logically reside. The events have a depth of no more than 3 levels (e.g. 4b(i) is a step with a depth of three levels). The construction of the series of events also involves an iterative process of "fitting" each of the steps into our generic trust model, and refining the steps if necessary. For some systems we have found it necessary to make assumptions about aspects of the system that are ambiguous, and they are stated before the listing of the series of events.

The next step of our analysis is to identify the entities that are relevant in the system in question. Referring to our generic Entity-Interaction model in section 3.2.4 we may identify two types of entities: *actors* who are either individuals or legal entities such as organisations, and *agents* that act on the actors' behalf. We recognise that some actors may not have agents acting on their behalf, and therefore in some systems we may not have agents for all the actors we identify.

Once we have identified the entities that are relevant to the system in question, we model the message flows among the entities using the Entity-Interaction model as discussed in section 3.2.4, and illustrate the message flows in a diagram similar to one in Figure 3-6. We also table the actions that happen in each of the steps and their associated messages. In this stage of the analysis we focus on the messages an entity sends to receives from another entity (i.e. messages that are external to the entity itself). Messages that are sent and received by the same entity (i.e. messages internal

to the entity itself) and messages that are ambiguous (i.e. messages that have an indefinite sender/receiver) are excluded from the analysis and are noted in our analysis. In this stage of our analysis we look for the specific implementation details and any notable characteristics about the system.

We then analyse the flow of messages for the system in question with respect to our generic trust model as illustrated in Figure 3-8. We also table the decisions that are made and their subsequent messages in each of the steps. In this stage of analysis we focus on messages that are sent from one component in our generic trust model (as depicted in Figure 3-8) to another component, that is, we exclude messages that are sent and received by the same component (i.e. messages internal to the component itself). Such internal messages will be noted in our analysis and their exclusion will be explained. In this stage of analysis we look at how the system in question manages trust, reputation and reciprocity information.

During the last stage of our analysis of the system with respect to our generic trust model we may find out that a particular system manages one type of information but not another. We may also find out that a particular system seems to manage a certain type of information, but its method of managing such information seems ambiguous from the system description or the series of events that we have constructed for system. Therefore we define the following categories of information management.

- A system manages a certain type of information (trust, reputation or reciprocity information) *internally* if the system in question indicates from our constructed series of events that it is directly involved in the creation and/or handling of such information (such as sending and receiving of messages).
- A system manages a certain type of information *externally* if the system in question indicates from our constructed series of events that it is not directly involved in the creation and/or handling of such information *and* the management of such information is done by processes *external* to the system in question, with contributions from the interactions within the system in question.

- A system does *not* manage a certain type of information if there is no information from the system description or from our constructed series of events that the system in question is involved in the creation or handling of such information.

We note that there are two possible explanations for a system not managing a certain type of information. Firstly the system may not be designed to handle such information, as the result some or all of the mechanisms required for the management of such information are not present in the system. Secondly the management of such information may be done through means that are external to the system itself, and therefore the management of such information is beyond the system's control.

4.2 Analysis of Systems

Using our generic trust model we conducted analysis on three online trading systems. Firstly we conducted our analysis on eBay, a popular online auction website with a feedback system for traders; secondly Kazaa, a popular file sharing network with a "integrity rating" system for the files; and lastly the Escrow Services System, a proposed mechanism for trading digital content for money among peers in a digital content marketplace.

4.2.1 eBay's Trader Feedback System

eBay (http://www.ebay.com/) is an E-Commerce website that allows auctions of various items to be conducted online. Registered users of eBay can sell items by starting auctions for those items, and buy items by participating and winning the bid in various auctions. People who want to trade at eBay are required to register themselves in eBay's system. A credit card number or an email address originated from a Internet Service Provider is required during the registration process as a proof of identity.

In addition to managing online auctions, eBay keeps a history of activities for all users at eBay. Information that is stored in the history includes all buying/selling transactions a user participated in (excluding unsuccessful bids), feedback and ratings made to the user by the counter-party of the transaction, and the user's response to that feedback. A subset of the information, namely transactions that have feedback reported on, the feedback itself and the response to that feedback (transactions that have no feedback are excluded), are made available to other users at eBay in the form

of a “User Feedback Report”. Figure 4-1 illustrates a web page displaying a report of such history and rating information. We will call such a report a *reputation report* for the remainder of this analysis. We note that these reputation reports from eBay are available to any person using the internet - they are not restricted to registered users of eBay.

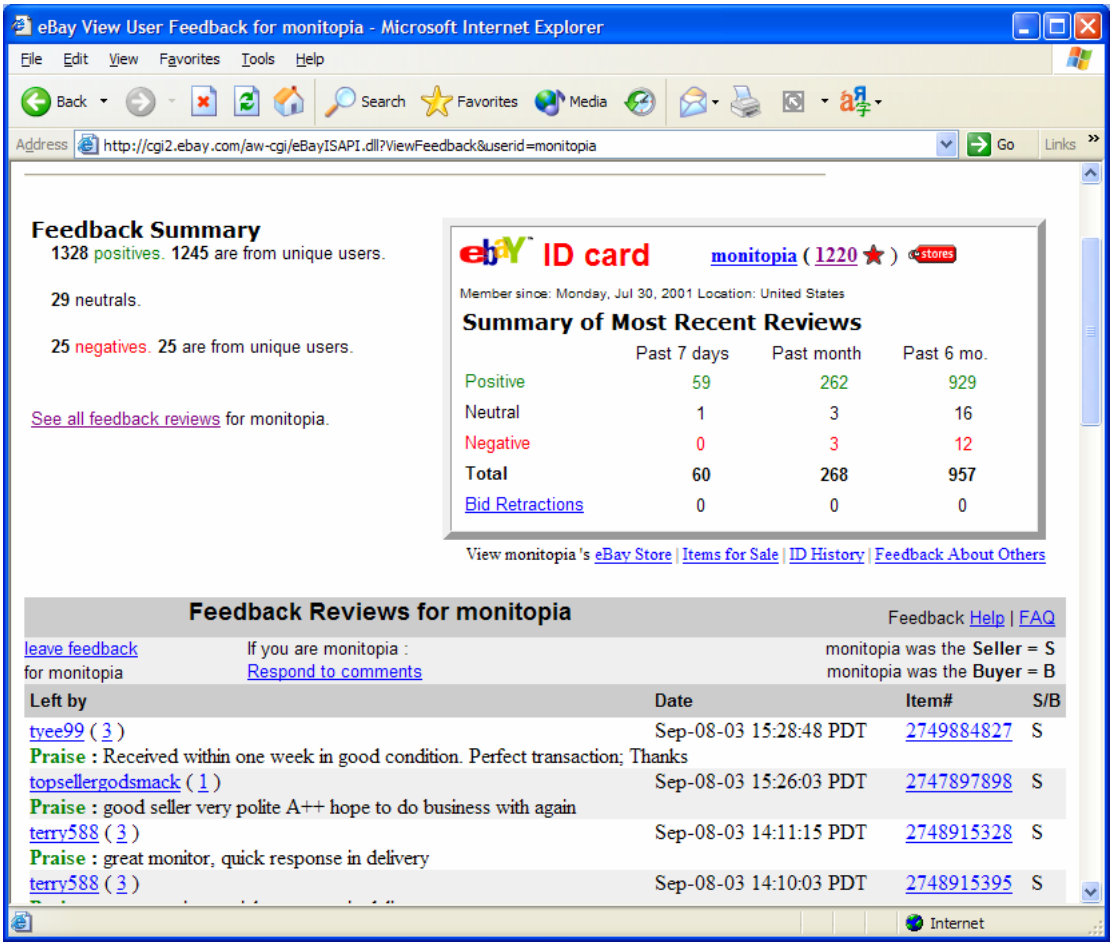


Figure 4-1 Web page displaying the transaction history and comments about eBay trader "monitopia" in both summary and detailed format. (Screenshot taken on 9 Sepember 2003)

There are a number of complementary services to the main auction and feedback system at eBay. Those services may or may not be operated by eBay but they are supported by eBay. Those services include escrow services which ensure delivery of payment and goods to the seller and buyer, and dispute resolution services which resolve conflicts between traders during a transaction. We will be focusing primarily on the auction and feedback system in our analysis.

4.2.1.1 Flow of Events in the eBay System

A set of simple instructions for buying and selling goods on eBay is available at its website [eBay 2004b, eBay 2004c]. The flow of events is described by eBay as follows:

Seller's Perspective:

1. **Find an item you want to sell.**
   Do some research on eBay to get an idea of your item's potential value and best category placement. Search for items similar to yours to find out what other seller's starting prices and categories were.
2. **List your item.**
   Click Sell in the navigation bar at the top of any eBay page. eBay's Sell Your Item form will take you through the process of listing your item step-by-step, including helping you find the correct category for your item.
3. **Set your price.**
   You can set a starting price and allow buyers to place bids, offer a fixed price you'll accept using Buy It Now, or both.
4. **Get paid!**
   When your listing ends, contact your winning buyer through email or by generating an eBay invoice within three business days. Let your buyer know the total price of the item, including your stated shipping costs, and how they can pay you. Offering PayPal allows your buyer to pay you quickly and easily.
5. **Ship the item.**
   After payment is received, send the item to the buyer's shipping address, specified with their payment or by email.
6. **Leave feedback.**
   After your successful sale, leave feedback for your buyer, and ask that they do the same.

[eBay 2004b]

Buyer's Perspective:

1. **Find an item.**
   Search by typing in a keyword for an item you're interested in, or browse through our categories.
2. **Learn about the item you found.**
   Read the item description carefully, and look at the pictures the seller has included. If you have any questions about the item that aren't answered in the item's description, you can ask the seller about the item by clicking on 'Ask Seller a Question' link. Carefully reading all the information and asking informed questions will help you determine if this is the item you want!
3. **Review the seller's feedback.**
   You can see the seller's feedback score and percentage of positive feedback right on the item page. Also, be sure and read the comments left by the seller's previous buyers to be sure that this is a seller you feel you can trust.
4. **Bid or Buy It Now.**
   Once you've found the item you want, you can place a bid or purchase the item instantly using Buy It Now. Some items are sold only in auction-style listings that require you to place a bid, while others include the Buy It Now option. This allows you to buy the item

instantly. Check the item page to see what purchase options are available to you.

5. **Pay for the item.**
   After you've won or purchased the item, send your payment to the seller. If the seller offers PayPal, clicking on the Pay Now button will allow you to pay quickly and easily with PayPal, eBay's preferred way to pay. Just check the seller's listing or email invoice to find out what the preferred payment method is and where you should send your payment.
6. **Leave feedback.**
   Here's your chance to tell the eBay community about your experience with this seller. You can leave feedback for any eBay member you've bought from or sold to.

[eBay 2004c]

In our analysis we constructed a series of events which may occur in the eBay system. This series of events has six major phases, and we identify the six phases from eBay's description of the events as follows:

1. Initiation Phase – This phase encapsulates the seller's "Find an item you want to sell", "List your item", "Set your price", buyer's "Find an item" and "Learn about the item you found" steps from eBay's description [eBay 2003b, eBay 2003c].
2. Trust Evaluation Phase – this phase encapsulates the buyer's "Review the seller's feedback" and "Bid or Buy It Now" steps from eBay's description.
3. Post-Auction Trader Notification Phase – This phase encapsulates the contacting part of the seller's "Get paid!" step and the contacting part of the buyer's "Pay for the item" step from eBay's description.
4. Transaction Completion Phase –This phase encapsulates the seller's "Ship the item" step and the payment part of the buyer's "Pay for the item" step from eBay's description.
5. Feedback Phase – This phase encapsulates the seller's and the buyer's "Leave feedback" steps from eBay's description.

Since the construction of this series of events is an iterative process of constructing the steps and attempting to "fit" the steps into our generic trust model, we find it appropriate to include our summary analysis in our series of events. We

provide our detailed analysis for the first phase to explain our rationale for the summary analysis.

1. Initiation Phase
    a. B. Seller, a registered user of eBay, decides to replace his professional home audio system with an even more professional set. He decides to sell his old system by auctioning it off at eBay. *(Our analysis: Process type is "Bob's Trust", outgoing message to "Bob's Reciprocity") – This is analogous to step 1a of our generic protocol for developing trust in section 3.2.5.2 (see page 51 for the complete protocol).*
    b. He creates an auction at eBay and opens the auction for bidding. *(Our analysis: Process type is "Bob's Reciprocity, outgoing message to "Sally's Reciprocity (eBay Auction Server)", data-store is "Bob's Memory of Outstanding Offers") – This is analogous to step 1b of our generic protocol.*
    c. A. Buyer, another registered user of eBay, is interested in buying a professional audio system second hand. She searches through the auction listings of audio systems at eBay *(Our analysis: Process type is "Alice's Reciprocity", outgoing message to "Sally's Reciprocity (eBay Auction Server)) – This is analogous to step 1c of your generic protocol.*
    d. eBay processes Alice's search query and returns a list of auction listings of audio systems, one of them being Bob's auction of his audio system. *(Our analysis: Process type is "Sally's Reciprocity (eBay Auction Server), outgoing message to "Alice's Reciprocity") – This is analogous to step 1d of our generic protocol.*

Step 1a in eBay's series of events is analogous to step 1a of our generic protocol as both steps involve a seller deciding to trade in some sort of online trading system. Thus the decision process in step 1a of eBay's series of event is categorised as "Bob's Trust", and its outgoing message of B. Seller's expectation to "Bob's Reciprocity"

Step 1b in eBay's series of events is analogous to step 1b of our generic protocol as both steps involve the seller creating an offer and making the offer available. Thus the offer creation process in step 1b of eBay's series of events is categorised as "Bob's Reciprocity", and its outgoing message of B. Seller's offer goes to "Sally's Reciprocity".

Step 1c in eBay's series of events is analogous to step 1c of our generic protocol as both steps involve the buyer searching or browsing the online trading system for possible trading activities to participate in (and in eBay's case it is auction activities). Thus the browsing process in step 1c in eBay's series of events is categorised as "Alice's Reciprocity", and its outgoing message of a request for available auction listings to "Sally's Reciprocity".

Step 1d in eBay's series of events is analogous to step 1d of our generic protocol as both steps involve the online trading system sending a list of available offers back to the would-be buyer. Thus the process of sending a list of offers in step 1d of eBay's series of events is categorised as "Sally's Reciprocity" and its outgoing message of the list of open auctions goes to "Alice's Reciprocity".

The remainder of the series of events and their summary analysis are as follows:

2. Trust Evaluation Phase
    a. Alice saw B. Seller's audio system being listed. She is interested in buying the audio system from B. Seller.:
        i. A. Buyer decides she needs to know more about B. Seller's reputation at eBay before considering whether she should participate in his auction. She requests B. Seller's reputation report from eBay. *(Our analysis: Process type is "Alice's Reciprocity", outgoing message to "Bob's Reputation", data-store is "Alice's Memory of Worthwhile Offers")*
        ii. eBay sends B. Seller's reputation report to A. Buyer. *(Our analysis: Process type is "Bob's Reputation", outgoing message to "Alice's Trust")*
    b. A. Buyer studies eBay's reputation report on B. Seller, and she perceives that B. Seller is reliable and completes transactions

on time, based on the feedback and ratings in the reputation report. A. Buyer concludes that B. Seller is a trustworthy trader. *(Our analysis: Process type is "Alice's Trust", outgoing message to "Alice's Reciprocity")*

c. Alice starts bidding in B. Seller's auction for the audio system. *(Our analysis: Process type is "Alice's Reciprocity", outgoing message to "Sally's Reciprocity (eBay Auction Server)")*

3. Post-Auction Trader Notification Phase
    a. B. Seller's auction for the audio system closes, and A. Buyer is the highest bidder for that auction. If the reserve price for B. Seller's auction has been met the following steps are carried out:
        i. eBay sends B. Seller a notification that his auction has met the reserve price and A. Buyer was the highest bidder for his auction, along with A. Buyer's contact details. *(Our analysis: Process type is "Sally's Reciprocity (eBay Auction Server)", outgoing message to "Bob's Reciprocity")*
        ii. eBay also sends A. Buyer a notification that she is the winning bidder for B. Seller's auction, along with B. Seller's contact details. *(Our analysis: Process type is "Sally's Reciprocity (eBay Auction Server)", outgoing message to "Alice's Reciprocity")*
        iii. eBay updates B. Seller's and A. Buyer's transaction history relating to auctions they participated. *(Our analysis: Process type is "Sally's Reciprocity (eBay Auction Server)", data-store is "Sally's transaction history database")*
    b. If the reserve price for B. Seller's auction has not been met when the auction closes then the following steps are carried out:
        i. eBay sends B. Seller a notification that his auction has not met the reserve price, and indicates that he may extend a "Second Chance Offer" to one of the bidders in

his auction. *(Our analysis: Process type is "Sally's Reciprocity (eBay Auction Server)", outgoing message to "Bob's Reciprocity")*

ii. eBay sends A. Buyer a notification that she was the highest bidder but the reserve price for B. Seller's auction was not met. *(Our analysis: Process type is "eBay's Auction Server", outgoing message to "Alice's Reciprocity")*

c. (Optional) At any stage B. Seller may request a reputation report about A. Buyer through the following steps:

i. B. Seller sends a request for A. Buyer's reputation report to eBay. *(Our analysis: Process type is "Bob's Reciprocity", outgoing message to "Alice's Reputation")*

ii. eBay responds by sending A. Buyer's reputation report to B. Seller. *(Our analysis: Process type is "Alice's Reputation, outgoing message to "Bob's Trust", data-store is "Sally's Reputation Database)*

iii. After studying A. Buyer's reputation report, B. Seller decides on a strategy for completing the transaction (such as payment before delivery, or the use of Escrow agents). *(Our analysis, Process type is "Bob's Trust", outgoing message to "Bob's Reciprocity", data-store is "Bob's Memory of 1st Hand Experience with Alice")*

4. Trader Communication Phase (Only one of 4a, 4b or 4c is executed)

a. If the reserve price for B. Seller's auction has been met (as per stage 3a) and B. Seller was the first to initiate contact with A. Buyer then the following steps will be carried out:

i. B. Seller contacts A. Buyer to discuss and finalise payment and delivery details for the audio system. *(Our analysis, Process type is "Bob's Reciprocity", outgoing message to "Alice's Reciprocity)*

ii. A. Buyer replies to B. Seller confirming the payment and delivery details. *(Our analysis: Process type is*

"Alice's Reciprocity", outgoing message to "Bob's Reciprocity")

b. If the reserve price for B. Seller's auction has been met (as per stage 3a) and A. Buyer was the first to initiate contact with B. Seller then the following steps will be carried out:
    i. A. Buyer contacts B. Seller to discuss and finalise payment and delivery details for the audio system. *(Our analysis: Process type is "Alice's Reciprocity", outgoing message to "Bob's Reciprocity")*
    ii. B. Seller replies to A. Buyer confirming the payment and delivery details. *(Our analysis, Process type is "Bob's Reciprocity", outgoing message to "Alice's Reciprocity)*
c. If the reserve price for B. Seller's auction has not been met (as per stage 3b) then B. Seller may decide to extend a "second chance offer" to A. Buyer:
    i. B. Seller notifies eBay that he is extending a second chance offer to A. Buyer, and does so through eBay's interface. *(Our analysis: Process type is "Bob's Reciprocity", outgoing message to "Sally's Reciprocity (eBay Auction Server)", data-store is "Bob's Memory of Outstanding Offers")*
    ii. eBay sends A. Buyer a notification that B. Seller is extending a second chance offer for the audio system to her. *(Our analysis: Process type is "Sally's Reciprocity (eBay Auction Server)", outgoing message to "Alice's Reciprocity")*
    iii. A. Buyer decides she will accept B. Seller's second chance offer and notifies eBay about the acceptance of the second chance offer. *(Our analysis: Process type is "Alice's Reciprocity", outgoing message to "Sally's Reciprocity (eBay Auction Server)")*
    iv. Upon receipt of A. Buyer's acceptance notification, eBay notifies B. Seller that A. Buyer has accepted his

second chance offer, along with her contact details. *(Our analysis: Process type is "Sally's Reciprocity (eBay Auction Server)", outgoing message to "Bob's Reciprocity")*

v. eBay also sends A. Buyer B. Seller's contact details upon receipt of her acceptance notification. *(Our analysis: Process type is "Sally's Reciprocity (eBay Auction Server)", outgoing message to "Alice's Reciprocity")*

vi. One of stages 4a or 4b follows, depending on which trader initiated the post-auction communication.

vii. eBay updates B. Seller's and A. Buyer's transaction history to relating to the trading of the audio system. *(Our analysis: Process type is "Sally's Reciprocity (eBay Auction Server)", data-store is "Sally's transaction history database")*

5. Transaction Completion Phase (Can be executed in any order)
    a. A. Buyer pays B. Seller for the audio system. *(Our analysis: Process type is "Alice's Reciprocity", outgoing message to "Bob's Reciprocity", data-store is "Alice's Memory of 1st Hand Experience with Bob")*
    b. B. Seller delivers the audio system to A. Buyer. *(Our analysis: Process type is "Bob's Reciprocity", outgoing message to "Alice's Reciprocity", data-store is "Bob's Memory of 1st Hand Experience with Alice")*
6. Feedback Phase (Can be executed in any order)
    a. A. Buyer subsequently visits eBay, and decides to provide some feedback and a rating about B. Seller with regard to the purchase of the audio system.
        i. A. Buyer sends her rating and feedback about B. Seller to eBay. *(Our analysis: Process type is "Alice's Reciprocity, outgoing message to "Bob's Reputation", data-store is "Alice's Memory of 1st Hand Experiences with Bob")*

ii. Upon receiving A. Buyer's feedbacks, eBay updates B. Seller's feedbacks, and notifies B. Seller about A. Buyer's newly-posted feedback. *(Our analysis: Process type is "Bob's Reputation", outgoing message to "Bob's Trust", data-store is "Sally's Reputation Database")*

b. B. Seller subsequently visits eBay, and decides to provide some feedback and a rating about A. Buyer as a buyer with regard to his sale of the audio system.

i. B. Seller sends his rating and feedbacks about A. Buyer to eBay. *(Our analysis: Process type is "Bob's Reciprocity, outgoing message to "Alice's Reputation", data-store is "Bob's Memory of 1st Hand Experiences with Alice")*

ii. After receiving B. Seller's feedbacks and rating, eBay notifies A. Buyer about B. Seller's newly-posted feedback. *(Our analysis: Process type is "Alice's Reputation", outgoing message to "Alice's Trust", data-store is "Sally's Reputation Database")*

4.2.1.2 Initial Analysis

From our series of events for eBay (outlined earlier in section 4.2.1.1) we tentatively identify the following entities in eBay. In our subsequent analysis of the activity in this trading system, later in this section, we will find that this identification leads to useful insights into how trust is established in eBay trading.

- A. Buyer being Alice, the trusting party.
- B. Seller being Bob, the trusted party.
- eBay being Sally, the trusted third party.
- eBay's auction system being Sally's agent, Sigma.

We do not model Alice and Bob as having agents acting on their behalf, although it is allowed in Figure 3-6 as most of the functionalities in eBay that are accessible by Alice and Bob require some form of human intervention.

Using the entities identified above, we diagram the flow of messages among the entities as illustrated in Figure 4-2.

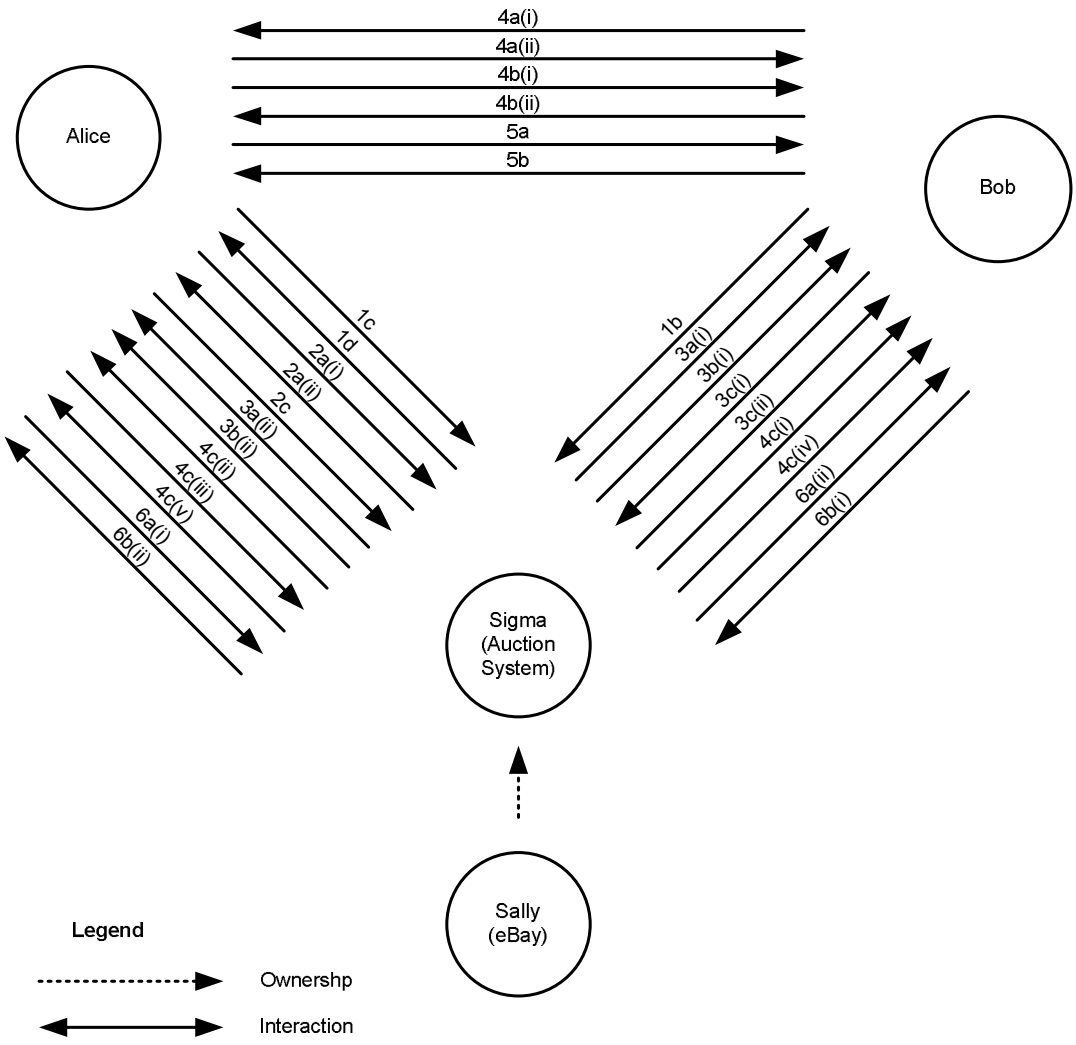


Figure 4-2 Diagram illustrating the message flow among Alice, Bob and eBay's agents.

We table the actions identified in each of the steps and their associated messages as illustrated in Table 4-1 and Table 4-2. Rows in grey indicate steps that are excluded from our message flow diagram in Figure 4-2.

Step	Action			Modelled Message (If Any)	
	Origin	Target	Description	Sender	Receiver
1a	B. Seller	B. Seller	B. Seller decides to sell his item at eBay	Bob	Bob
1b	B. Seller	eBay	B. Seller creates an auction at eBay	Bob	Sigma
1c	A. Buyer	eBay	A. Buyer searches through eBay's listings	Alice	Sigma
1d	eBay	A. Buyer	eBay sends Alice a list of auctions	Sigma	Alice
2a(i)	A. Buyer	eBay	A. Buyer requests B. Seller's Reputation Report	Alice	Sigma
2a(ii)	eBay	A. Buyer	eBay's response for A. Buyer's reuqest for Reputation Report	Sigma	Alice
2b	A. Buyer	A. Buyer	A. Buyer decides that B. Seller is trustworthy	Alice	Alice
2c	A. Buyer	eBay	A. Buyer places her bid in B. Seller's Auction at eBay	Alice	Sigma
3a(i)	eBay	B. Seller	eBay notifies B. Seller that his auction has met the reserve price	Sigma	Bob
3a(ii)	eBay	A. Buyer	eBay notifies A.Buyer that she is the winning bidder for B. Seller's auction	Sigma	Alice
3a(iii)	eBay	eBay	eBay updates A. Buyer's and B.Seller's transaction history	Sigma	Sigma
3b(i)	eBay	B. Seller	eBay notifies B. Seller that his auction did not meet the reserve price	Sigma	Bob
3b(ii)	eBay	A. Buyer	eBay notifies A.Buyer that she placed the highest bid but the reserve price was not met	Sigma	Alice
3c(i)	B. Seller	eBay	B. Seller requesting A.Buyer's reputation report	Bob	Sigma
3c(ii)	eBay	B. Seller	eBay responds B. Seller's request for Reputation Report	Sigma	Bob
3c(iii)	B. Seller	B. Seller	B. Seller deciding on a strategy for completing the transaction	Bob	Bob
4a(i)	B. Seller	A. Buyer	B. Seller contacts A.Buyer to finalise transaction details	Bob	Alice
4a(ii)	A. Buyer	B. Seller	A. Buyer confirming transaction details	Alice	Bob

Table 4-1 Table illustrating the actions and messages associated with the hypothetical scenario in eBay

Step	Action			Modelled Message (If Any)	
	Origin	Target	Description	Sender	Receiver
4c(i)	B. Seller	eBay	B. Seller extends a Second Chance offer to A. Buyer through eBay	Bob	Sigma
4c(ii)	eBay	A. Buyer	eBay notifies A. Buyer of B. Seller's Second Chance Offer	Sigma	Alice
4c(iii)	A. Buyer	eBay	A. Buyer notifies eBay of her acceptance of B. Seller's Second Chance Offer	Alice	Sigma
4c(iv)	eBay	B. Seller	eBay sends B. Seller A. Buyer's contact details	Sigma	Bob
4c(v)	eBay	A. Buyer	eBay sends A. Buyer B. Seller's contact details	Sigma	Alice
4c(vi)	N/A	N/A	A. Buyer and B. Seller contact each other to finalise the transaction	N/A	N/A
4c(vii)	eBay	eBay	eBay updates A. Buyer's and B.Seller's transaction history	Sigma	Sigma
5a	A. Buyer	B. Seller	A. Buyer pays B. Seller for the goods	Alice	Bob
5b	B. Seller	A. Buyer	B. Seller delivers the goods to A. Buyer	Bob	Alice
6a(i)	A. Buyer	eBay	A. Buyer sends her feedback about B. Seller to eBay	Alice	Sigma
6a(ii)	eBay	B. Seller	eBay notifies B. Seller of A. Buyer's new feedback	Sigma	Bob
6b(i)	B. Seller	eBay	B. Seller sends his feedback about A. Buyer to eBay	Bob	Sigma
6b(ii)	eBay	A. Buyer	eBay notifies A. Buyer of B. Seller's new feedback	Sigma	Alice

Table 4-2 Table illustrating the actions and messages associated with the hypothetical scenario in eBay (continued)

Steps 1a, 3a(iii), 3c(iii) and 4c(ii) are excluded from Figure 4-2 as the messages associated with those steps are internal messages to the sender (i.e. the sender and the receiver of the message are the same entity). Step 4c(vi) is excluded from Figure 4-2 because the contents and the direction of the associated messages depend on the precise order of communication when Alice and Bob finally made contact to each other.

We conduct our analysis on the reputation category relating to Bob as a trader. We diagrammed the flow of messages with respect to the generic model in Figure 4-3.

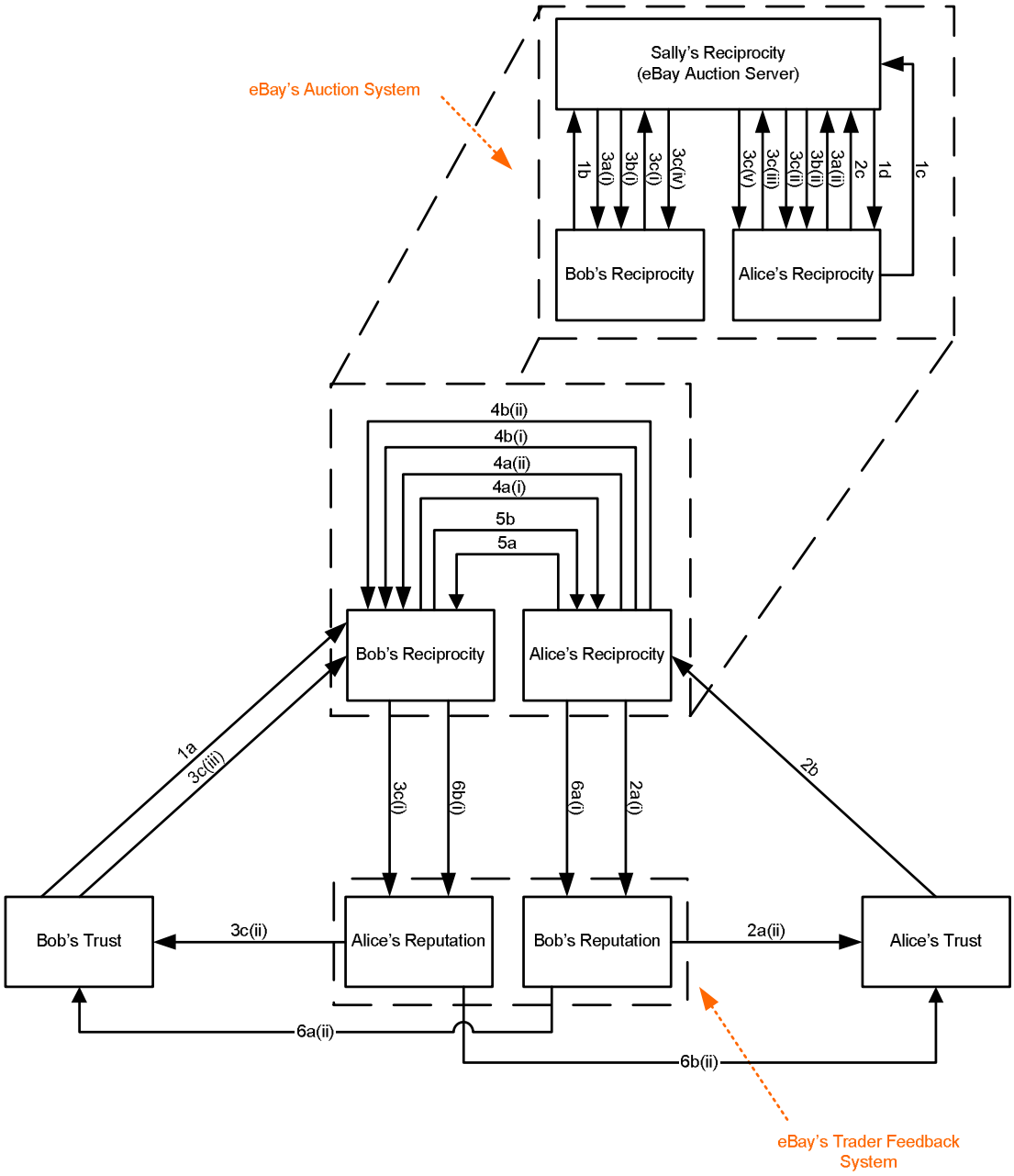


Figure 4-3 Diagram illustrating the flow of messages in eBay with respect to the generic trust model

The rationales for our modelling of the message flows in eBay with respect with the generic trust model are as follows:

- In Step 1a, Bob decides and offers to engage in a specific reciprocity, namely an auction at eBay. Bob would not do this unless he has sufficient trust in eBay. Thus we model the decision-making message of Step 1a as going from "Bob's Trust" to "Bob's Reciprocity",

- In Step 1b Bob creates an offer and makes the offer available for bidding. Thus we model the auction-creation message as going from "Bob's Reciprocity" to "Sally's Reciprocity (eBay Auction Server)".
- In step 1c Alice goes searching in eBay for possible auctions for her to participate in. Thus we model the search listings message as going from "Alice's Reciprocity" to "Sally's Reciprocity (eBay Auction Server)".
- In step 1d eBay sends Alice a list of open auctions that fits her search criteria. Thus we model this auction listings message as going from "Sally's Reciprocity (eBay Auction Server)" to "Alice's Reciprocity".

The remainder of our modelling rationales are provided in section 6.2 of the Appendix.

From Figure 4-3 it is evident that eBay's trader feedback system manages reputation information about Alice and Bob, as both Alice and Bob can post feedbacks and ratings about each other through eBay (steps 6a(i) and 6b(i)), and eBay records such feedbacks and ratings. As a result Alice's and Bob's reputation in eBay persists after the transaction (as Alice is able obtain Bob's transaction history) and carries on to future transactions (both Alice's and previous traders' feedbacks on Bob are stored in eBay's database). We therefore conclude that eBay's trader feedback system manages reputation information internally.

We also conclude that eBay manages reciprocity internally for the managing of auction listings and the running of auctions. This is reflected in our analysis of steps 1b, 1c, and 1d. See Figure 4-3, where step 1b (Bob's creation of the auction) is modelled as going from "Bob's Reciprocity" to "Sally's Reciprocity (eBay Auction Server)". Step 1c (Alice requesting the auction listings fromeBay) is modelled as going from "Alice's Reciprocity" to "Sally's Reciprocity (eBay Auction Server)". Step 1d (eBay returning a list of auction listings) is modelled as going from "Sally's Reciprocity (eBay Auction Server)" to "Alice's Reciprocity".

It is evident from our series of events that eBay does not manage reciprocity information internally for the managing of transaction completions (steps 5a and 5b) when Bob and Alice actually exchange goods and services, as it is explicitly left to the transacting parties to make arrangements for (both in steps 4a(i), 4a(ii), 4b(i) and

4b(ii) of our series of events and in eBay's brief buying/selling instructions [eBay 2004b, eBay 2004c]). This is reflected in our analysis in Figure 4-2 and Figure 4-3, as the steps concerning the transaction completion phase (steps 5a and 5b) are modelled as messages going between Alice and Bob (in Figure 4-2) and between "Alice's Reciprocity" and "Bob's Reciprocity" (in Figure 4-3) without intervention or mediation from eBay.

There is no evidence, either from our series of events or from our analysis in Figure 4-3, that eBay's trader feedback system manages trust information internally. From our analysis eBay's trader feedback system only provides reputation information to user in helping them to make their trust decisions; it does not make any conclusions or suggestions of whether a certain user is trustworthy or otherwise.

4.2.1.3 In Depth Analysis

We note that eBay's auction system and its trader feedback system are centralised systems (as opposed to a peer-to-peer implementation) with respect to auction listings and data storage. All the auction information and feedback information are stored in eBay's servers and does not reside in the users' computers. This is evident as Alice and Bob are required to communicate with eBay's systems in steps 1, 2, and 3 of our series of events in order to browse auction listings and obtain trader feedback information in the form of a reputation report.

Although eBay has a lot of involvement in the phases of auction listing, running of auctions and traders' feedback, it has very little involvement at the transaction completion phase. This is evident in steps 4a(i), 4a(ii), 4b(i), 4b(ii), 5a and 5b of our series of events when Alice and Bob communicate directly to each other without mediation or intervention from eBay.

However we also note that Second Chance Offers are conducted with heavy intervention from eBay. We conclude the heavy involvement from eBay in second chance offers is due to the fact that commissions are charged against Bob if the second chance offer is accepted by Alice. This is evident in steps 4c(i) through to 4c(v) in our series of events where eBay mediates all the communications between Alice and Bob during the process of offering and accepting the second chance offer.

We also note that while Alice has the ability of examining Bob's reputation before she decides on whether she will trade with Bob in eBay, Bob does not have the same privilege. Once Bob's auction has met the reserve price Bob has the obligation,

as described in eBay's Terms and Conditions, to complete the transaction (except in some rare circumstances where Bob – or even Alice – can cancel the transaction altogether). Therefore unless the auction did not meet the reserve price (in which case Bob can pick the bidders he wants to send the Second Chance Offers to) Bob is "stuck" with Alice from the point the auction closes.

We note that from our analysis in Figure 4-3 Alice and Bob go around the trust cycle once. Alice starts her trust cycle from "Alice's Reciprocity" (step 1c and 2a(i)), goes to "Bob's Reputation" (step 2a(ii)), then to "Alice's Trust" (step 2b), then back to "Alice's Reciprocity" (step 2c, steps 4 and 5a) and she stops her cycle at "Bob's Reputation" (step 6a(i)). Bob start his trust cycle from "Bob's Trust" (step 1a), goes to "Bob's Reciprocity" (step 1b), then to "Alice's Reputation" (step 3c(ii)), then back to "Bob's Trust" (step 3c(iii)), then to "Bob's Reciprocity" (steps 4 and 5), and he stops his cycle at "Alice's Reputation" (step 6b(i)). We note that Bob has the choice of not going through his part of the trust cycle as he can choose whether to inspect Alice's reputation for his reciprocation with her (the steps in 3c are optional flows).

If Alice and Bob are initially unknown to each other, the first time they go through the trust cycle will provide an initial value to each other's reputation (as they both enquire about each other's reputation through the trader feedback system), as well as firsthand experiences of the other's reciprocation. Subsequent visits to the trust cycle by Alice and Bob (once they have known each other) refresh their perceptions to each other's reputation (as they enquire about each other's updated reputation) as well as gaining new experiences from their reciprocations.

In addition Alice and Bob can be uniquely identified in eBay, as their aliases are unique within eBay. Thus we conclude that eBay's trader feedback system facilitate the development of interpersonal trust.

4.2.2 The Kazaa File Sharing Network

Kazaa (http://www.kazaa.com/) is a peer-to-peer program which allows files to be shared across the internet. Users of Kazaa can search for files to download, and also provide files that will be shared among other users. Users are required to provide an alias (or pseudonym) in order to participate in the Kazaa network. Users have total freedom to choose what files they would like to share with others (to the extent of choosing which directories they will share the files from), and the freedom to choose whether they want to share files with others. Although it was designed to support the sharing of any type of files, Kazaa is primarily used by users to trade music and video files.

Since Kazaa does not require the existence of centralised servers, its network of nodes is formed by certain users acting as "supernodes". The role of the supernodes is to manage a list of files being shared by the non-supernode users within close proximity (the list is uploaded by the non-supernode user upon connecting to the supernode), to process search queries by non-supernode users, and to process search queries relayed by other supernodes (as user search queries can be processed more efficiently by having the supernodes relaying queries only among themselves).

From version 2.0 of Kazaa a feature called "Integrity Rating" was added into the program. With the "Integrity Rating" feature users can provide ratings to files concerning their quality and relevance of its metadata (information about the file such as file size, artist, description etc) to the actual content. This "Integrity Rating" feature is our main focus of analysis of Kazaa as a "trust" system. Figure 4-4 shows an instance of a search result listing with some of the files rated by users. The listing was produced using the keyword "Dido" with the "P2P Search" and "audio" options selected. Such integrity rating information about the files being shared is stored in the users' individual computers, rather than on a centralised location.

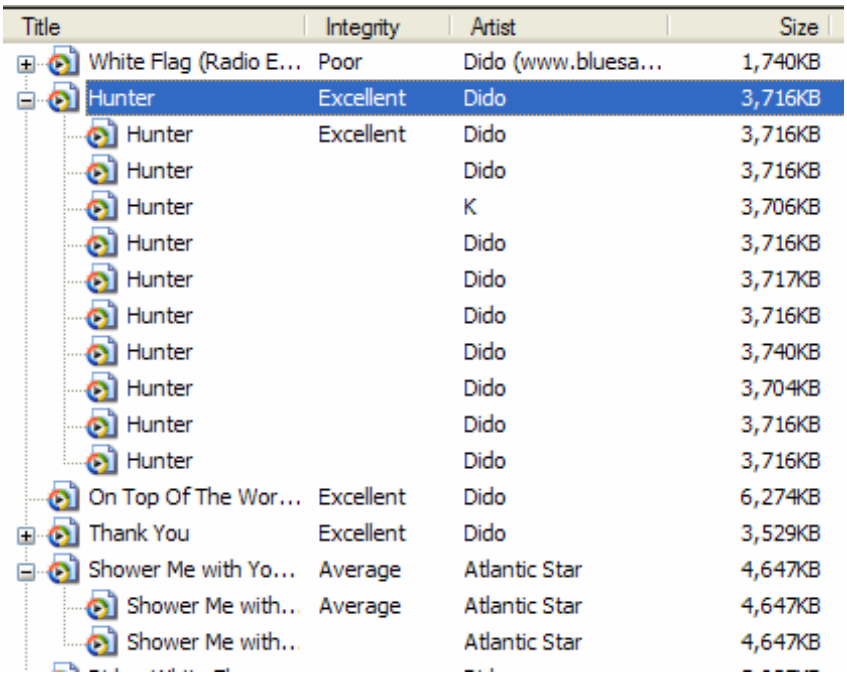


Figure 4-4 An instance of the search result list in Kazaa Lite.

In early 2002 Kazaa was alleged to be shipped with spyware – programs that keep track of the user's online activity and submit those results to online marketing agencies without the user's explicit consent. As the result a group of enthusiasts distributed a modified version of Kazaa with the spyware removed. This no-spyware version of Kazaa, known as Kazaa Lite or K-Lite (http://www.zeropaid.com/kazaalite/) is used for our analysis.

4.2.2.1 Flow of Events in Kazaa

We have constructed the following series of events for our analysis of Kazaa's Integrity Rating system:

0. Initiation Phase
    a. B. Sharer decides to participate in a file sharing network. After trying out several file sharing applications he decides to stick with the Kazaa file sharing network. *(Our analysis: process type is "Bob's Trust", outgoing message to "Bob's Reciprocity")*
    b. B. Sharer compiles a list of files that he wants to share with other user, and using the Kazaa client application he provides comments and rating for each of the files he shares. *(Our*

analysis: process type is "Bob's Reciprocity", data-store is "Bob's Memory of Outstanding Offers")

c. B. Sharer connects to the Kazaa network with his Kazaa client and submits the list of files he is sharing to the supernode he is connected to. *(Our analysis: process type is "Bob's Reciprocity", outgoing message to "Sally's Reciprocity (Kazaa Supernode)")7*

1. "A. Downloader goes browsing" Phase
    a. A. Downloader wants to obtain a digital copy of the song "White Flag" by the artist Dido and she decides to look for the song in the Kazaa network:
        i. A. Downloader connects to its nearest supernode with her Kazaa client application and searches for the song using her Kazaa client with the keyword "Dido" and limits the list of results to audio files by choosing the "audio" option. *(Our analysis: process type is "Alice's Reciprocity", outgoing message to "Sally's Reciprocity (Kazaa Supernode)")*
        ii. The supernode which A. Downloader's Kazaa client is connected to begins to process A. Downloader's search query. After searching for matches in its own list files shared by its connected users the supernode sends A. Downloader's query to other supernodes. *(Our analysis: process type is "Sally's Reciprocity (Kazaa supernode)", internal message to itself)*
        iii. The other supernodes processes A. Downloader's query and submits the results back to the supernode A. Downloader is connected to. *(Our analysis: process type is "Sally's Reciprocity (Kazaa supernode)", internal message to itself)*
        iv. The supernode which A. Downloader is connected to returns a list of matches for her search query. The information on that list includes the title of the song, the artist of the song, file size, length of the song, sound

quality of the song in terms of bit rate, the estimated amount of time required to download the file, the users with possession of the file, and the integrity of the file. *(Our analysis: process type is "Sally's Reciprocity (Kazaa Supernode)", outgoing message to "Alice's Reciprocity")*

b. A. Downloader navigates the list of search results, and finds multiple entries with the title "White Flag". These entries have different file sizes, but the metadata is similar in general. Due to the number of possible entries in the search results list A. Downloader decides to look at the integrity ratings of the search results.
    i. A. Downloader requests the search results to be sorted by integrity rating by clicking on the integrity rating heading in the search results pane in the Kazaa client. *(Our analysis, process type is "Alice's Reciprocity", outgoing message to "Bob's Reputation")*
    ii. A. Downloader's Kazaa client sorts the search results listing becomes by integrity rating, starting from the "excellent", to "good", "average", "poor" and finally the entries with no integrity ratings. After sorting the search results A. Downloader's Kazaa client displays the results back to A. Downloader. *(Our analysis: process type is "Bob's Reputation", outgoing message to "Alice's Trust")*

c. Upon looking at the integrity rating of the entries in the search results listing A. Downloader discovers that one of the entries has an integrity rating of "excellent" attached to it. After reviewing the metadata of the file with the "excellent" integrity rating attached to it A. Downloader decides that she will download the file in question on the evidence of the integrity rating and the relevance of the file's metadata. *(Our analysis: process type is "Alice's Trust", outgoing message to "Alice's Reciprocity")*

2. File Transfer Phase
    a. Using the Kazaa client application, A. Downloader sends file download requests for the file “Dido - White Flag.mp3” to the users with possession of the file. *(Our analysis: process type is “Alice’s Reciprocity”, outgoing message to “Bob’s Reciprocity”)*
    b. Upon receipt of A. Downloader’s file download request the other users’ Kazaa client allocation determines whether they should start the file transfer with A. Downloader’s Kazaa client, based on the configurations set by their respective owners.
        i. If the other user’s Kazaa client decides to accept A. Downloader’s download request it will respond by sending a “download request accepted” message to A. Downloader’s Kazaa client, in which case A. Downloader’s Kazaa client will start receiving the file (or portions of the file) from that particular user. *(Our analysis: process type is “Bob’s Reciprocity”, outgoing message to “Alice’s Reciprocity”)*
        ii. If the other user’s Kazaa client decides not to accept A. Downloader’s download request (due to reasons such as bandwidth limitations, or the user’s Kazaa client is already serving the maximum number of download requests), it will respond by sending a “download request declined” message back to A. Downloader’s Kazaa client. *(Our analysis: process type is “Bob’s Reciprocity”, outgoing message to “Alice’s Reciprocity”)*
3. Post-Transfer Evaluation Phase
    a. When the file “Dido – White Flag.mp3” has been completely downloaded, A. Downloader evaluates the file by playing it in her favourite media player. A. Downloader decides that the file is of excellent quality, she then gives the file an “excellent” integrity rating. *(Our analysis: process type is “Alice’s Reciprocity”)*

b. A. Downloader's Kazaa client synchronize the list of files A. Downloader's is currently sharing along with the updated integrity ratings with the supernode it is connected to. *(Our analysis: process type is "Alice's Reciprocity", outgoing message to "Bob's Reputation")*

4.2.2.2 Initial Analysis

From the series of events mentioned in section 4.2.2.1 we identify two main issues with entities identification. Firstly Alice may download the files in segments from multiple sources, and this implies the possibility that there exists more than one B. Sharer. Secondly although Alice is connected to only one supernode, her search query is propagated among other supernodes in the Kazaa network, thus this implies the existence of multiple supernodes in the Kazaa network.

Taking into account the issues mentioned above we tentatively identify the following entities in Kazaa In our subsequent analysis of the activity in this trading system, later in this section, we will find that this identification leads to useful insights into how trust is established in the Kazaa network.

- A. Downloader being Alice, the trusting party.
- A. Downloader's Kazaa client being Alice's agent, Alpha.
- Bob, the trusted party, is the set {Bob_1, Bob_2 ... Bob_n} of all file sharers {B. $Sharer_1$, B. $Sharer_2$, … B. $Sharer_n$} with possession of the file A. Downloader is seeking.
- Beta, Bob's agent, is the set {$Beta_1$, $Beta_2$ … $Beta_n$} of all instances of Kazaa clients Bob is running on their respective computers.
- Sally, the trusted third party, is the set {$Sally_1$, $Sally_2$ … $Sally_n$} of all persons running the Kazaa client as a supernode.
- Sigma, Sally's agent, is the set {$Sigma_1$, $Sigma_2$ … $Sigma_n$} of all instances of Kazaa clients (being run as supernodes) that Sally is running of their respective computers.

We assume that the elements in the set of all Bob's are mapped one-to-one to the elements in the set of all Betas (i.e. Bob_1 runs $Beta_1$, Bob_2 runs $Beta_2$ etc.), that the

elements in the set of all Sally's are mapped one-to-one to the elements in set of all Sigma's (i.e. $Sally_1$ runs $Sigma_1$, $Sally_2$ runs $Sigma_2$ etc.). We also assume that Alice's agent Alpha is connected specifically to $Sigma_1$.

From our series of events for the Kazaa network we have diagrammed the flow of messages among entities as illustrated in Figure 4-5.

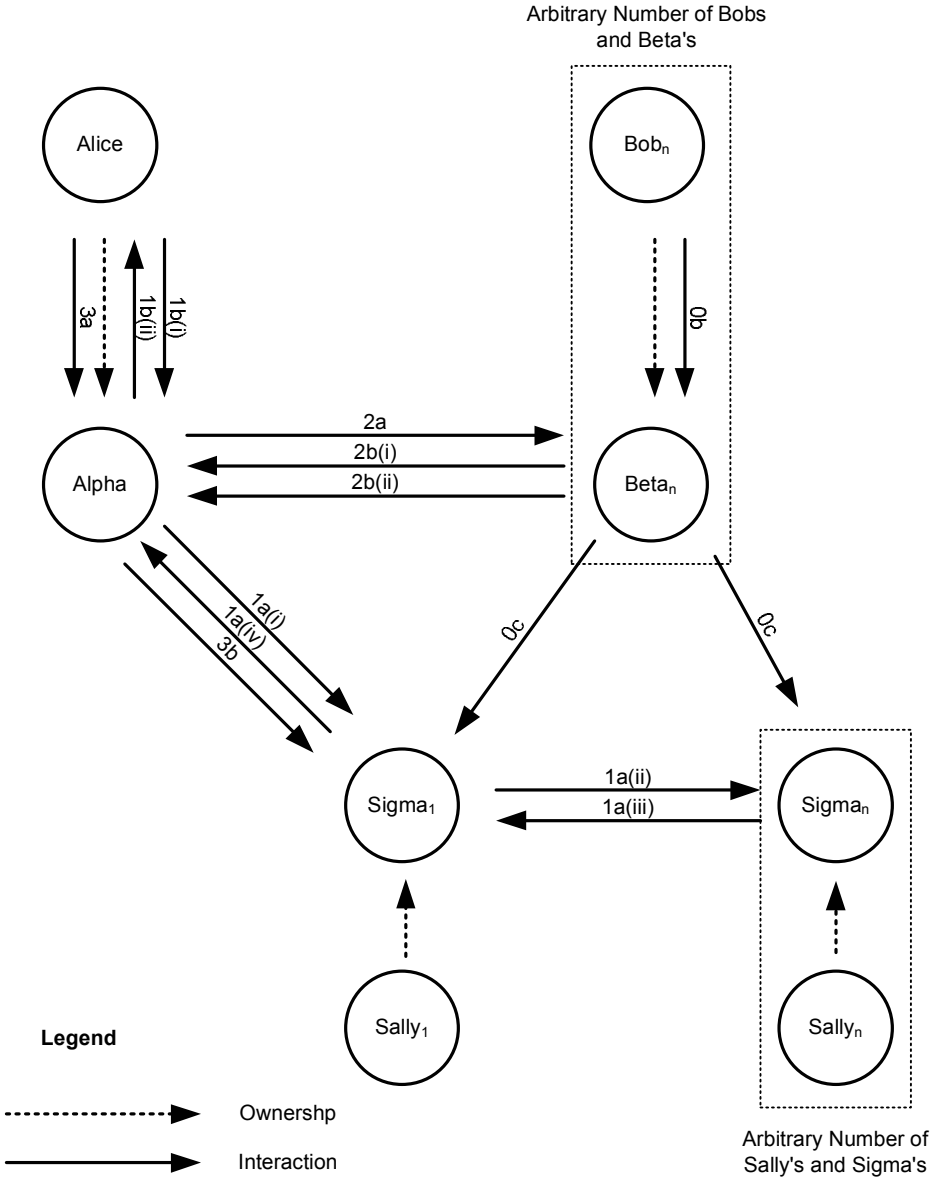


Figure 4-5 Diagram illustrating the flow of message among entities in the Kazaa network

We table the actions identified in each of the steps and their associated messages as illustrated in Table 4-3. Entries that are greyed out are steps that are not present in Figure 4-5.

Step	Action			Modelled Message (If Any)	
	Origin	Target	Description	Sender	Receiver
0a	B. Sharer	B. Sharer	B. Sharer decides to share files in the Kazaa network	Bob(n)	Bob(n)
0b	B. Sharer	B. Sharer's Kazaa Client	B. Sharer compiles a list of files to be shared in the Kazaa network and provides ratings for each of the files	Bob(n)	Beta(n)
0c	B. Sharer's Kazaa Client	Kazaa Network	B. Sharer submits his list of downloadable files to the Kazaa network	Beta(n)	Sigma(n)
1a(i)	A. Downloader's Kazaa Client	Kazaa Network	A. Downloader searches the Kazaa network for files through her Kazaa client	Alpha	Sigma(1)
1a(ii)	Kazaa Network	Kazaa Network	A. Downloader's connected supernode progagates her query to other supernodes	Sigma(1)	Sigma(n)
1a(iii)	Kazaa Network	Kazaa Network	The other supernodes sends A. Downloader's query results back to A. Downloader's supernode	Sigma(n)	Sigma(1)
1a(iv)	Kazaa Network	A. Downloader's Kazaa Client	A. Downloader's connected supernode return the search query results back to A. Downloader.	Sigma(1)	Alpha
1b(i)	A. Downloader	A. Downloader's Kazaa Client	A. Downloader requests her Kazaa client to sort the search query results by integrity rating	Alice	Alpha
1b(ii)	A. Downloader's Kazaa Client	A. Downloader	A. Downloader's Kazaa client sorts the search query results by integrity rating	Alpha	Alice
1c	A. Downloader	A. Downloader	A. Downloader decides to download a file based on the file's integrity rating	Alice	Alice
2a	A. Downloader	B. Sharer	A. Downloaders sends s file download request to the B. Sharer's with possession of the file	Alpha	Beta(n)
2b(i)	B. Sharer	A. Downloader	B. Sharer decides to accept A. Downloader's request and proceed with the file transmission	Beta(n)	Alpha
2b(ii)	B. Sharer	A. Downloader	B. Sharer declines A. Downloader request	Beta(n)	Alpha
3a	A. Downloader	A. Downloader's Kazaa Client	A. Downloader provides an integrity rating for thenewly downloaded file	Alice	Alpha
3b	A. Downloader's Kazaa Client	Kazaa Network	A. Downloader's Kazaa client synchornises her list of downloadable files with its connected supernode	Alpha	Sigma(1)

Table 4-3 Table illustrating the actions and messages associated with the hypothetical scenario in Kazaa

Step 0a is excluded from our diagram in Figure 4-5 as the associated message is internal within Bob himself (Bob is both the sender and the recipient of the message), and he does not communicate with other identified entities in our analysis.

Step 1c is excluded from our diagram in Figure 4-5 as the associated message is internal within Alice (Alice is both the sender and the recipient of the message), and does not communicate with other identified entities in our analysis.

We also diagram the flow of messages with respect to the generic model in Figure 4-6. The messages in grey indicate messages in our original generic model in Figure 3-8 that we are unable to map onto messages in the Kazaa trading system. In Section 4.2.2.3 we discuss some of the external processes that handle these missing (grey) messages.

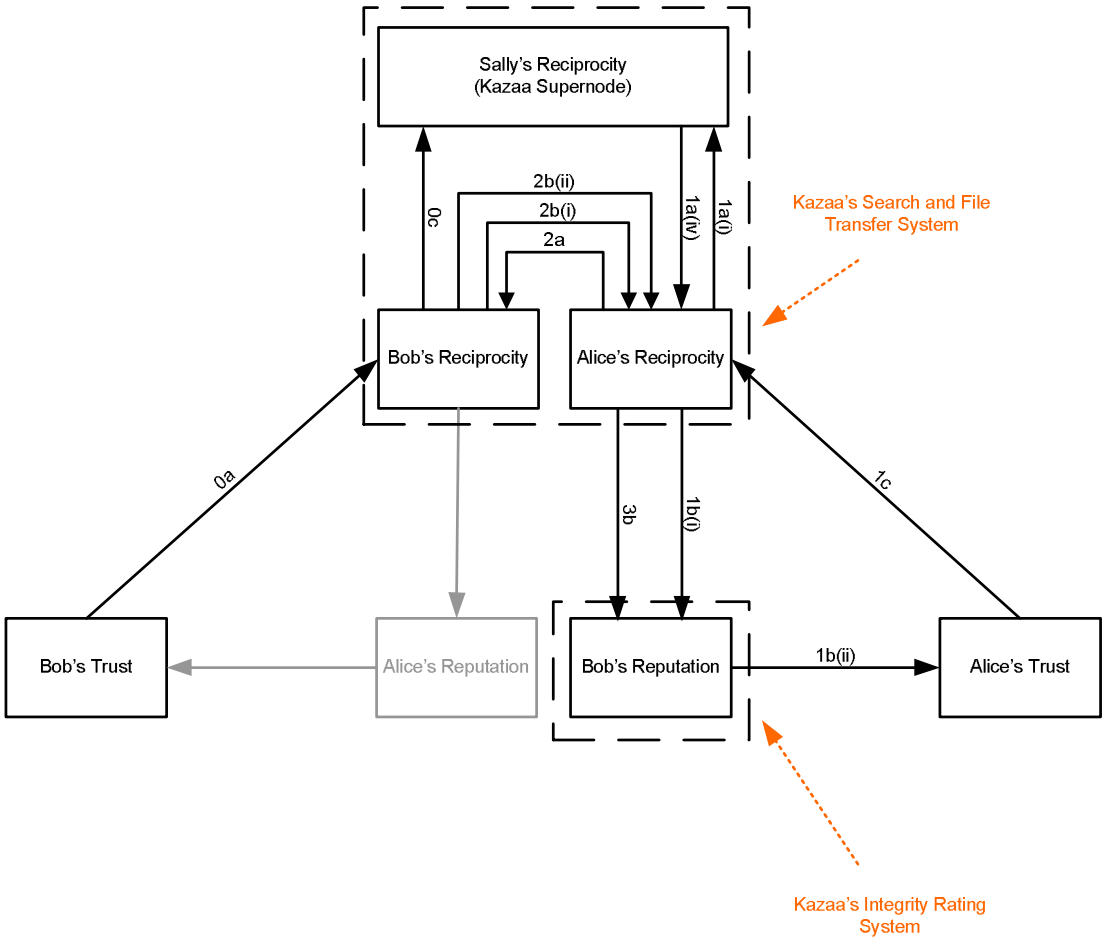


Figure 4-6 Diagram illustrating the flow of messages in Kazaa with respect to the generic model

The rationales for our modelling of the message flows in the Kazaa network with respect with the generic trust model are as follows:

- In step 0a, Bob decides to share his files in the Kazaa network. Bob would not do this unless he has sufficient trust in the Kazaa network. Thus we model the decision-making message as going from Bob's Trust to "Bob's Reciprocity".
- In step 0b, Bob applies integrity ratings to the files he is sharing in the Kazaa network. Thus we model the apply-integrity-rating message as one internal to "Bob's Reciprocity" (which is excluded from our diagram in Figure 4-6).
- In step 0c, Bob's Kazaa client submits to his connected supernode the list of files Bob is currently sharing. Thus we model this downloadable-files-list message as going from "Bob's Reciprocity" to "Sally's Reciprocity (Kazaa Supernode)".

The remainder of the rationales for our modelling of the message flows with respect to the generic trust model is provided in section 6.3 of the Appendix.

We conclude that Kazaa manages reciprocity internally for both facilitating search queries and file transfers. From the system description and our analysis in Figure 4-6 it is evident that Kazaa's Supernodes are heavily involved in facilitating search queries, as the messages concerning search queries (steps 1a(i) to 1a(iv)) flow from, to, and within "Sally's Reciprocity (Kazaa Supernode)". The evidence for Kazaa's internal management of file transfers lies in steps 2a, 2b(i) and 2b(ii) in our series of events, where Alice and Bob facilitate file transfers through their respective Kazaa clients. Although Kazaa's supernodes are not involved the actual file transfers (as steps 2a, 2b(i) and 2b(ii) does not flow from or to "Sally's Reciprocity (Kazaa Supernode)"), the fact that Bob's Kazaa client can choose to accept or decline Alice's file transfer request (in steps 2b(i) and 2b(ii)) implies that the Kazaa client manages file transfers on their user's behalf.

We conclude that Kazaa manages reputation information internally for managing integrity ratings on the files. This is evident in steps 1b(i), 1b(ii) and 3b of our series of events and our analysis in Figure 4-6. Step 1b(i) is modelled as going from "Alice's Reciprocity" to "Bob's Reputation". Step 1b(ii) is modelled as going from "Bob's Reputation" to "Alice's Trust". Step 3b is modelled as going from "Alice's Reciprocity" to "Bob's Reputation".

We conclude that Kazaa does not manage trust information internally as there is no evidence from our series of events that Kazaa provides such information for Alice suggesting whether Bob (or a particular file) is trustworthy or otherwise. From our analysis Kazaa's integrity rating system only provides reputation information in the form of a reputation report for helping users in deciding whether to download a particular file or otherwise; it does not make any suggestions or conclusions as to whether a particular file is worth downloading or not.

4.2.2.3 In Depth Analysis

We note that Kazaa utilises a distributed architecture similar to one used by Domain Name Services (DNS hereafter). In DNS systems when a client submits a domain name query to a DNS server, the DNS server in question will firstly attempt to resolve the query into an IP address on its own, and if it cannot resolve the query to an IP address with its available information, it will propagate the query to other DNS servers to resolve the query. After the DNS query is resolved, the client connects directly to the server in question with the resolved IP address.

In Kazaa when a user submits a search query to a supernode, the supernode in question first processes the query on its own using the lists of downloadable files that other connected users have submitted to the supernode, after which the supernode will propagate the search query to other supernodes in the Kazaa network, and returns those results to the user as it receives the results from the other supernodes. After the search query has been processed, the user requests the file he/she wants to download directly from the user(s) with possession of the file. This is evident in steps 1a(ii) to 1a(v) of our series of events, where $Sigma_1$ propagates Alice's query to other Sigmas currently connected to the Kazaa network, and returns the search results from the other Sigma's back to Alice as the query results arrive back to $Sigma_1$.

We also observe that while Kazaa's supernodes have a lot of involvement in the processing search queries, it have no involvement with the actual file transfers. This is evident in steps 1a(i) to 1a(iv), step 2a, 2b(i) and 2b(ii) of our series of events. In steps 1a(i) to 1a(iv) (when Alice searches the Kazaa network for files) messages related to Alice's search queries flows between Alpha and $Sigma_1$, and among the Sigma's themselves. However none of the messages in steps 2a, 2b(i) and 2b(ii) (when Alice requests the file from the other users) goes to any of the Sigma's.

While the integrity rating system in Kazaa supports both positive and negative feedback for files, we found that from a practical standpoint it s inadequate in providing negative feedback. The rating information is stored in the user's computer for each file they rated, and is only present as long as the file is still present in the user's computer (i.e. a file's rating information is basically lost if the file is deleted or is moved to a location different to the designated "sharing directories"). This suggests that for the rating of a poorly-rated file to be shown in search results the file itself must be present in one of the user's sharing directories.

However, from a practical standpoint there is little point for a user to keep those poorly-rated files on his computer other than for providing feedback for other Kazaa users or for archival purposes. In most cases the user would simply delete the files in question, thus creating a lack of negative feedback in the Kazaa network.

We looked at whether the mechanisms present in the Kazaa network facilitate the development of interpersonal trust. For this part of the analysis we have made two observations.

Firstly although the Sigmas provide some sort of reputation report for Alice when they process her search query, the source information from which the reputation report is compiled with is stored in each of the Bobs' computers rather than in the Sigmas themselves (which stores the information temporarily over the time when Bob is connected to the Kazaa network). In addition because the search results contains files that were available within a certain proximity at a single point in time, this means the same search query executed at a different time or different location may yield different results. Thus the information in the reputation report changes over time and location.

Secondly Alice has no means of providing feedback or ratings about any particular user in the Kazaa network. This is firstly due to the peer to peer nature of the Kazaa network. This means that there isn't a reliable place where rating information about a particular user can be stored, as the Sigmas may go online or offline at any time. Secondly Bob's alias may be changed easily by going through the options menu in the Kazaa client, making the association between real-world identities and online aliases a rather weak one. Thirdly aliases are not unique in Kazaa, making uniquely identifying a specific Bob a difficult task.

From the above observations we conclude that the integrity rating system in Kazaa does not facilitate the development of interpersonal trust, as the mechanisms

and the weak association of individuals to aliases currently present in Kazaa are inadequate for the facilitation to be reified.

While the Integrity Rating system in Kazaa does not facilitate the development of interpersonal trust, it does implicitly facilitate the development of institutional trust between the file downloaders and the file sharers. The development of institutional trust in Kazaa is facilitated through the usage its file sharing capabilities.

If we generalise Alice as a universe of all file downloaders and Bob as the universe of all file sharers in the Kazaa network, then using our generic trust model in Figure 3-8 we can explain each of the process components with respect to the development of institutional trust between Alice and Bob.

Alice's cycle of the Trust model:

- Alice's Reciprocity – The downloading of files made available by the file sharers.
- Bob's Reputation – The reputation of the sharers in the Kazaa network for sharing desired files and files of good quality.
- Alice's Trust –The downloaders trust that they will find what they want from the sharers in the Kazaa network and that the sharers will not "spam" the network with junk files.

Bob's cycle of the Trust model:

- Bob's Reciprocity – The sharing/uploading of files to the downloaders.
- Alice's Reputation – The reputation of the downloaders in the Kazaa network for being "ordinary" computer users (and not working for government agencies or "industry associations" such as the RIAA or the MPAA)
- Bob's Trust – The trust that the sharers have in the anonymity of their identities in the Kazaa network and that the downloaders are indeed ordinary computer users.

While the types of messages flowing from "Alice's Trust" to "Alice's Reciprocity" for the development of institutional trust will be similar to those modelled in our series of events in Section 4.2.2.1, we envisage that in addition to

integrity rating messages there also exist “word of mouth” messages going from “Alice’s Reciprocity” to “Bob’s Reputation” that are external to the Kazaa network itself. Such “word of mouth” messages might exist as part of a verbal conversation, or it might exist as messages posted in a private bulletin board or public forum. As a result, for the development of institutional trust, the reputation reports in messages going from “Bob’s Reputation” to “Alice’s Trust” will include external feedback from the Alices in addition to the integrity ratings submitted by Alice.

For the development of institutional trust, we envisage that there exist feedback messages going from “Bob’s Reciprocity” to “Alice’s Reputation”. Such messages will be external to the Kazaa network, and exist as verbal comments in a conversation or in written form such as posts in a bulletin board or public forum. We envisage a lack of feedback being made against Alice (as there is little incentive for Bob to provide feedback about Alice’s downloading activities), and that the lack of negative feedback actually develops Alice’s reputation in a positive manner (i.e. “No news is good news”). Examples of negative feedbacks against Alice include news about a subpoena being served against Bob’s internet service provider (as the existence of the subpoena exposes the fact that some of the Alices are working for government agencies or industry associations).

In addition to feedback messages going from “Bob’s Reciprocity” to “Alice’s Reputation”, we envisage that there exist messages going from “Alice’s Reputation” to “Bob’s Trust” in the development of institutional trust. Such messages are also external to the Kazaa network, and takes the form of reputation reports consisting of oral accounts of Bob’s experiences as a file sharer and news concerning the file sharing network (such as subpoenas being served to extract identities of file sharers in the Kazaa network). Such reports affect Bob’s expectation in both their anonymity in the Kazaa network and trust in Alice as being ordinary file downloaders, thus affecting his participation levels in the Kazaa network (for existing users it is whether to share more/less files; for new users it is whether to start sharing files in the Kazaa network). Such expectations can be modelled as messages going from “Bob’s Trust” to “Bob’s Reciprocity”, thus completing Bob’s trust cycle in the development of institutional trust.

4.2.3 A Proposed Escrow Services System for P2P Trading Networks

The Escrow Services System was proposed by Hone et al [Horne 2001] to provide a mechanism for content providers (the *senders*) in a peer-to-peer environment to serve content and receive remunerations for serving that content, and for users (the *receivers*) to ensure that the downloaded content is what they have asked for and is of good quality.

The system employs a Trusted Third Party which is named as the Escrow Server to participate in every transaction that occurs within the system. The main functionality of the system involves both ensuring that the user gets the content he/she wants and that the content providers get their payment for providing the content to the user. The system uses a combination of encryption and a collision-resistant hash function to provide the functionalities claimed by its authors.

The authors proposed two schemes for their escrow services system: the basic scheme which requires the sender to communicate with the escrow server during the content preparation stage to send his hash values (which is used for content verification), and the second scheme which does not require the sender to establish any connection with the escrow server at all. We conducted our analysis on the basic scheme of the escrow services system.

One of the challenges that we faced in the course of our analysis was the lack of information in the system's originating conference paper. The authors provided extensive information about the transmission mechanisms of the escrow server (as it was the main focus of the paper) and the possibilities it provides for the other components of a complete trading system. However they have provided little detail in terms of the requirements that the other components might need to have in order to have the escrow transmission mechanism incorporated into a complete trading system. We will discuss the issue in detail in our analysis.

4.2.3.1 Flow of Events in the Escrow Services System

We have made the following assumptions for our analysis of the escrow services system:

- A centralised digital content marketplace/directory service exists in our system (the paper claims that escrow services transmission mechanism can be implemented as part of a centralised or distributed directory service).

- This digital content marketplace uses the escrow services transmission mechanism exclusively as their transaction completion method of choice, thus the marketplace and the escrow services system are tightly integrated.
- Some form of reputation management mechanism is present in our digital content marketplace. This reputation management mechanism is capable of aggregating reputation information and producing reputation reports about the content providers in the system. We also assume that only buyers of digital content may submit feedbacks (on either the content provider or the digital content itself, depending on specific implementations of the marketplace). This reputation management mechanism does not aggregate or distribute reputation information on the content buyers in the system.

We do not make assumptions on the type of digital content that this marketplace is catered for, nor we make assumptions on the types of information the reputation report is comprised from. This is due to the fact that the authors did not design the transmission mechanism with a specific type of digital content in mind, and that the usefulness of the types of information to be used in the reputation report varies, depending on the type of digital content the marketplace is catered for.

The following series of events is constructed for our analysis of the escrow services system:

0. Content Preparation Stage
    a. B. Sender decides to sell copies of some content *C* to other users in the Escrow Services system. *(Our analysis: process type is "Bob's Trust", outgoing message to "Bob's Reciprocity")*
    b. B. Sender decides on the price *Pr(C)* for content *C* for which he is willing to serve *C* for. He also prepares a description $D_B(C)$ for content *C*, an encrypted version $E_K(C)$ of content *C*, using key *K*, and computes the hash $H_B(E_K(C))$ of the encrypted

content $E_K(C)$. *(Our analysis: process type is "Bob's Reciprocity", internal message to itself)*

c. B. Sender transmits the key *K*, the hash value $H_B(E_K(C))$, the description $D_B(C)$ and the price $Pr(C)$ of *C* to the escrow server. *(Our analysis: process type is "Bob's Reciprocity", outgoing message to "Sally's Reciprocity (Escrow Server)", data-store is "Bob's Memory of Oustanding Offers")*

d. The ES notifies the digital content marketplace that B. Sender is serving the content *C*, and sends B. Sender's description $D_B(C)$ for the marketplace's "product listing". *(Our analysis: process type is "Sally's Reciprocity (Escrow Server), outgoing message to "Sally's Reciprocity (Digital Content Marketplace)")*

1. "A. Receiver goes shopping" Stage

   a. A. Receiver browses the digital content marketplace for content of interest:

      i. She submits her request for a list of contents and their prices that are available to the digital content marketplace. *(Our analysis: process type is "Alice's Reciprocity", outgoing message to "Sally's Reciprocity (Digital Content Marketplace)")*

      ii. The digital content marketplace sends to A. Receiver a list of digital contents that are available for trading, one of them being Bob's content *C* which is being serving for price $Pr(C)$. *(Our analysis: process type is "Sally's Reciprocity (Digital Content Marketplace)", outgoing message to "Alice's Reciprocity")*

   b. A. Receiver is interested in buying content *C* from B. Sender after looking at his description $D_B(C)$ of *C*. A. Receiver decides that she needs to know more about B. Sender's reputation at the marketplace before notifying B. Sender of her interest in getting content *C*:

      i. A. Receiver requests B. Sender's reputation report from the digital content marketplace. *(Our analysis: process*

type is "Alice's Reciprocity", outgoing message to "Bob's Reputation", data-store is "Alice's Memory of Worthwhile Offers")

ii. The digital content marketplace responds by sending A. Receiver the reputation report about B. Sender. *(Our analysis: process type is "Bob's Reputation", outgoing message to "Alice's Trust")*

c. After studying B. Sender's reputation report, A. Receiver perceives that B. Sender has an acceptable reputation, and decides that she will obtain the content from B. Sender. *(Our analysis: process type is "Alice's Trust", outgoing message to "Alice's Reciprocity")*

d. A. Receiver contacts B. Sender about the purchase of his digital content *C*. *(Our analysis: process type is "Alice's Reciprocity", outgoing message to "Bob's Reciprocity")*

2. Transaction finalisation and Content Transfer Stage

a. A. Receiver and B. Sender negotiate and finalise the terms of the transaction. The terms include the price *Pr(C)* for which A. Receiver will pay for the content, and the description of the content *C*:

i. B. Sender sends A. Receiver his preferred terms for the transaction. *(Our analysis: process type is "Bob's Reciprocity", outgoing message to "Alice's Reciprocity")*

ii. A. Receiver accepts B. Sender's terms for the transaction. *(Our analysis: process type is "Alice's Reciprocity", outgoing message to "Bob's Reciprocity")*

b. After A. Receiver and B. Sender agree on the terms of the transaction, one of the following may happen.

i. If the terms of the transaction bind B. Sender to a specific file *C*, B. Sender is required to provide in advance a commitment $Com_B(C)$ to content *C* or the hash *H(C)* of the content to A. Receiver. *(Our analysis:*

process type is "Bob's Reciprocity", outgoing message to "Alice's Reciprocity")

ii. If the terms of the transaction do not bind B. Sender to any specific file or files then continue to the next step.

c. B. Sender sends the encrypted content $E_K(C)$ to A. Receiver.

3. Content Verification Stage

a. A. Receiver computes her version of the hash $H_A(E_K(C))$ for the encrypted content $E_K(C)$. *(Our analysis: process type is "Alice's Reciprocity", internal message to itself)*

b. A. Receiver sends $H_A(E_K(C))$ along with her description $D_A(C)$ of content C, the payment $Pay_A(C)$ for the content and information $ID(B)$ about B. Sender's identity to the escrow server. *(Our analysis: process type is "Alice's Reciprocity", outgoing message to "Sally's Reciprocity (Escrow Server)")*

c. The escrow server compares A. Receiver's hash value $H_A(E_K(C))$ with B. Sender's hash value $H_B(E_K(C))$, A. Receiver's description $D_A(C)$ with B. Sender's description $D_B(C)$, and A. Receiver's payment $Pay_A(C)$ with B. Sender's asking price $Pr(C)$. *(Our analysis: process type is "Sally's Reciprocity (Escrow Server)", internal message to itself)*

d. Depending on the results of the comparison one of the following occurs:

i. If all of the hash values, descriptions and the payment/price pair are equal then the escrow server verifies that A. Receiver's payment $Pay_A(C)$ is valid. *(Our analysis: process type is "Sally's Reciprocity (Escrow Server)", internal message to itself)*

ii. If any one of the hash values, descriptions or the payment/price pair does not equal then the escrow server notifies A. Receiver with a failure message $Failure(H_A(E_K(C)))$ indication that the hash values do not match, in which case A. Receiver is not required to pay, and the transaction ends here. *(Our analysis:*

process type is "Sally's Reciprocity (Escrow Server)", outgoing message to "Alice's Reciprocity")

4. Payment Verification Stage
    a. After the escrow server has sent A. Receiver's payment $Pay_A(C)$ for verification, one of the following may happen depending on the verification result:
        i. If A. Receiver's payment $Pay_A(C)$ is valid, the escrow server sends A. Receiver a success message $Success(H_A(E_K(C)))$ indicating that the encrypted content $E_K(C)$ she received from B. Sender is valid, and sends her the key K to decrypt the content. *(Our analysis: process type is "Sally's Reciprocity (Escrow Server)", outgoing message to "Alice's Reciprocity")*
        ii. If A. Receiver's payment $Pay_A(C)$ is not valid, then the transaction ends here.
    b. If A. Receiver's Payment $Pay_A(C)$ is valid, the escrow server processes the payment and sends a notification message to B. Sender indicating that A. Receiver's payment $Pay_A(C)$ to him has been processed. *(Our analysis: process type is "Sally's Reciprocity", outgoing message to "Bob's Reciprocity")*
5. Post transaction feedback stage
    a. After A. Receiver receives (from step 4a(i)) the success message $Success(H_A(E_K(C)))$ and the decryption key K for decrypting the encrypted digital content $E_K(C)$. A. Receiver evaluates the digital content C. *(Our analysis: process type is "Alice's Reciprocity", internal message to itself)*
    b. After her evaluation of the digital content she submits her feedback to the digital content marketplace. *(Our analysis: process type is "Alice's Reciprocity", outgoing message to "Bob's Reputation")*

4.2.3.2 Initial Analysis

From the series of events mentioned earlier we tentatively identify the following entities in the escrow services system:

- A. Receiver as Alice, the trusting party.
- B. Sender as Bob, the trusted party.
- The company that runs the digital content marketplace and the escrow services as Sally, the trusted third party.
- The digital content marketplace as Sally's agent, $Sigma_1$.
- The escrow server as Sally's agent, $Sigma_2$.

Using the entities identified earlier we diagram the flow of messages among them as illustrated in Figure 4-7. We note that $Sigma_1$ (the digital content marketplace) and messages that flow into and out from the entity are in green to indicate that they exist as a result of our assumption of its presence made earlier.

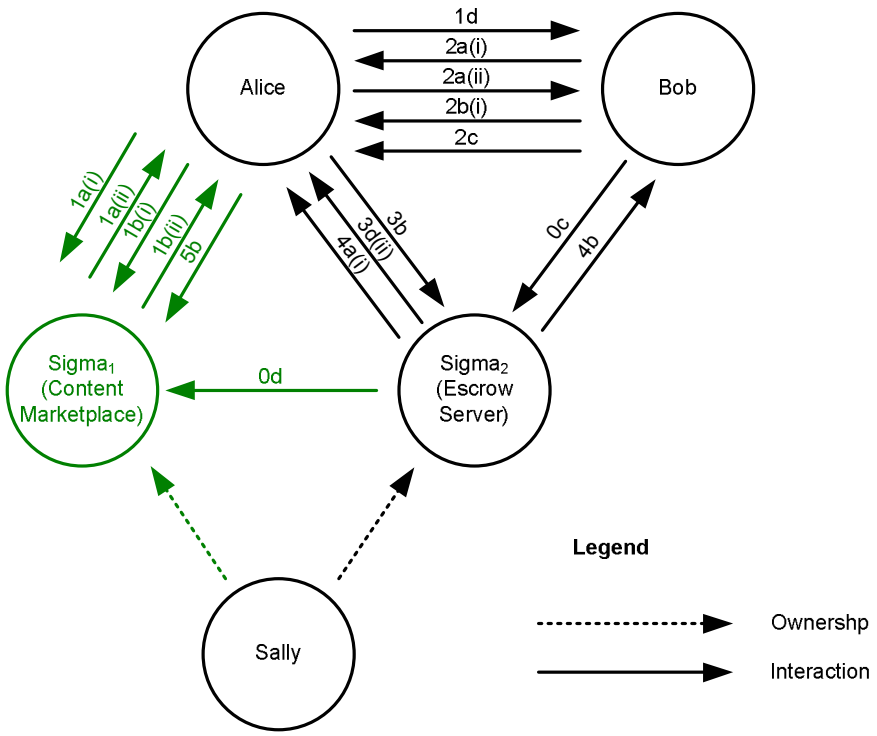


Figure 4-7 Diagram illustrating the flow of messages among entities in the Escrow Services System

We have tabled the actions and the associated messages in each of the steps in our series of events as illustrated in Table 4-4 and Table 4-5. Steps that are greyed out indicate steps that are excluded from our diagram in Figure 4-7. Steps that are shown in green indicate messages that are present as the result of our assumption of the existence of a digital content marketplace ($Sigma_1$) in our system.

Step	Action			Modelled Message (If Any)	
	Origin	Target	Description	Sender	Receiver
0a	B. Sender	B. Sender	B. Sender decides to make some digital content available for trading	Bob	Bob
0b	B. Sender	B. Sender	B. Sender prepares the description, encrypts the content, and computes the hash of the encrypted content	Bob	Bob
0c	B. Sender	Escrow Server	B. Sender sends the description, hash, the decryption key and price of the digital content to the escrow server	Bob	Sigma(2)
0d	Escrow Server	Digital Content Marketplace	The Escrow Server notifies the digital content marketplace of the availability of B. Sender's digital content	Sigma(2)	Sigma(1)
1a(i)	A. Receiver	Digital Content Marketplace	A. Receiver requests the digital content marketplace for available content listing	Alice	Sigma(1)
1a(ii)	Digital Content Marketplace	A. Receiver	The digital content marketplace sends to A. Receiver a list of availabe content	Sigma(1)	Alice
1b(i)	A. Receiver	Digital Content Marketplace	A. Receiver requests athe reputation report on B. Sender	Alice	Sigma(1)
1b(ii)	Digital Content Marketplace	A. Receiver	The digital content marketplace sends to A. Receiver B. Sender's reputation report	Sigma(1)	Alice
1c	A. Receiver	B. Sender	A. Receivers decides to trust B. Sender and contacts him about the purchase of the digital content	Alice	Bob
2a(i)	B. Sender	A. Receiver	B. Sender sends to A. Receiver his preferred terms of transaction	Bob	Alice
2a(ii)	A. Receiver	B. Sender	A. Receiver accepts B. Sender's terms of transaction	Alice	Bob
2b(i)	B. Sender	A. Receiver	B. Sender advances a commitment to the digital content to A. Receiver	Bob	Alice
2b(ii)	NA	NA	No action is taken in this step		
2c	B. Sender	A. Receiver	B. Sender sends the encrypted version of the digital content to A. Receiver	Bob	Alice

Table 4-4 Table illustrating the actions and messages associated with the hypothetical scenario in the Escrow Services System

Step	Action			Modelled Message (If Any)	
	Origin	Target	Description	Sender	Receiver
3a	A. Receiver	A. Receiver	A. Receiver computes her hash of the encrypted digital content	Alice	Alice
3b	A. Receiver	Escrow Server	A. Receiver sends her computed hash, her description of the digital content B. Sender's identity, and payment to the Escrow Server	Alice	Sigma(2)
3c	Escrow Server	Escrow Server	Escrow Server compares the hashes, descriptions, the price and payment	Sigma(2)	Sigma(2)
3d(i)	Escrow Server	Escrow Server	Escrow Server verifies that A. Receiver's payment is valid	Sigma(2)	Sigma(2)
3d(ii)	Escrow Server	A. Receiver	Escrow Server notifies A. Receiver that her hash of the encrypted does not match the one computed by B. Sender	Sigma(2)	Alice
4a(i)	Escrow Server	A. Receiver	Escrow Server notifies A. Receiver that her hash of the encrypted content matches the one computed by B. Sender and sends her the decryption key	Sigma(2)	Alice
4a(ii)	NA	NA	No action is taken		
4b	Escrow Server	B. Sender	Escrow Server notifies B. Sender that A. Receiver's payment has been processed successfully	Sigma(2)	Bob
5a	A. Receiver	A. Receiver	A.Receiver decrypts the encrypted content and evaluates the digital content	Alice	Alice
5b	A. Receiver	Digital Content Marketplace	A. Receiver posts some feedback about Bob to the digital content marketplace	Alice	Sigma(1)

Table 4-5 Table illustrating the actions and messages associated with the hypothetical scenario in the Escrow Services System (continued)

Steps 0a and 0b are excluded from Figure 4-7 as Bob is both the sender and recipient of the associated messages in those steps. Steps 3a and 5a are excluded from Figure 4-7 as Alice is both the sender and the recipient and associated message in those steps. Similarly steps 3c and 3d(i) are excluded from our diagram in Figure 4-7 as $Sigma_2$ is both the sender and the recipient of the payment-verification message in that step. Steps 2b(ii) and 4a(ii) are not present in our diagram in Figure 4-7 as no action took in those steps.

We diagram the flow of messages between Alice, Bob and the escrow server with respect to the generic model in Figure 4-8. The entities and messages in green indicate entities and messages that exist as a result of our assumptions, and the messages in grey indicate messages that do not exist in our generic trust model in

Figure 3-8 but we think are significant in the Escrow Services System. We discuss the significance of those messages in our in depth analysis in Section 4.2.3.3.

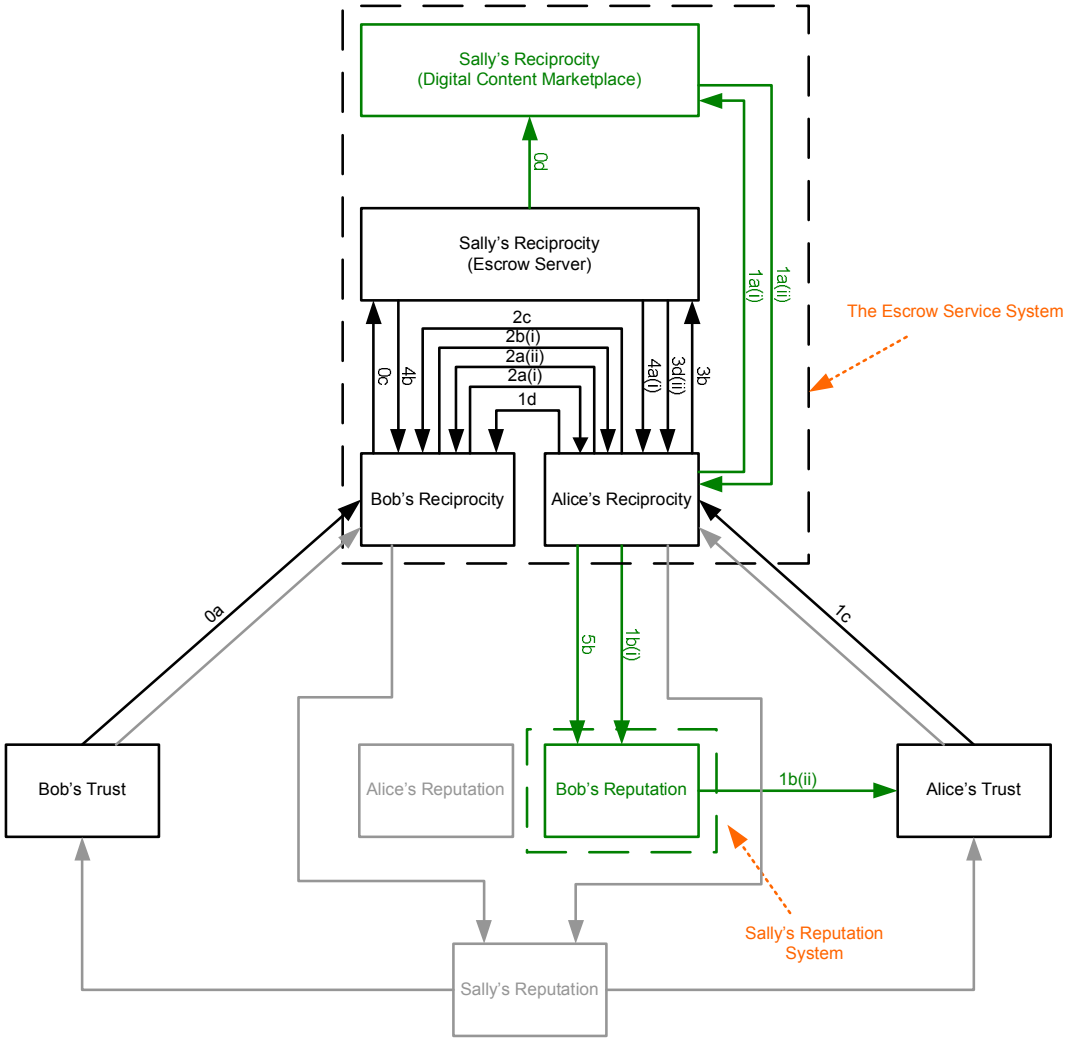


Figure 4-8 Flow of messages between Alice, Bob and the escrow server with respect to the generic model in the Escrow Services System

We hereby provide our rationale for the modelling of the message flows in Figure 4-8 with respect to our generic trust model:

- In step 0a, Bob decides and offers to engage in a specific reciprocity, namely to sell copies of his digital content *C* in the digital content marketplace. Bob would not do this unless he has sufficient trust in the marketplace. Thus we model the decision-making message as going from "Bob's Trust "to "Bob's Reciprocity".

- In steps 0b, Bob decides on the price *Pr(C)* for which he is selling copies of digital content *C* for, and prepares a description $D_B(C)$, an encrypted version $E_K(C)$ of *C*, and a hash $H_B(E_K(C))$ of the encrypted content. In this step Bob engages in a specific reciprocity of preparing for his sale of his digital content. Thus we model these preparation messages as messages internal within "Bob's Reciprocity", and therefore are excluded from our diagram illustrated in Figure 4-8.
- In step 0c, Bob sends the price *Pr(C)*, the decryption key *K*, the hash $H_B(E_K(C))$ of the encrypted content $E_K(C)$ and the description $D_B(C)$ to the escrow server. Thus we model this new-content-info message as going from "Bob's Reciprocity" to "Sally's Reciprocity (Escrow Server)".
- In step 0d, the escrow server sends a notification to the digital content marketplace about Bob's newly-submitted content. Thus we model this new-content-available message as going from "Sally's Reciprocity (Escrow Server)" to "Sally's Reciprocity (Digital Content Marketplace)".

The remainder of the rationale for the modelling of message flows with respect to the generic trust model is available in section 6.4 of the Appendix.

From our analysis we conclude that the Escrow Services transmission mechanism manages reciprocity internally for the transfer of digital content and payment to the buyer and content provider respectively. This is reflected in our analysis of steps 3b, 3c, 3d(i), 3d(ii), 4a(i), and 4b. See Figure 4-8, where step 3b (Alice's submission of her hash to the escrow server) modelled as going from "Alice's Reciprocity" to "Sally's Reciprocity (Escrow Server)". Step 3c (The escrow server's comparison of the hashes) is modelled as a "Sally's Reciprocity (Escrow Server)" process. Step 3d(i) (Escrow server's sending of payment for verification) is modelled as a "Sally's Reciprocity (Escrow Server)" process. Step 3d(ii) (Escrow server's failure message to Alice) is modelled as going from "Sally's Reciprocity (Escrow Server)" to "Alice's Reciprocity". Step 4a(i) (Escrow Server's success message to Alice) is modelled as going from "Sally's Reciprocity (Escrow Server)" to

"Alice's Reciprocity". Step 4b (Escrow server's notification to Bob) is modelled as going from "Sally's Reciprocity (Escrow Server)" to "Bob's Reciprocity".

There is no evidence, either from our series of events of from our analysis in Figure 4-8 that the Escrow Service system manages reciprocity information internally for the digital content listings in the digital content marketplace. Although we have assumed that the digital content marketplace exists in our system, the most fundamental messages involving the browsing of digital content listings in steps 1c and 1d are modelled as going between "Alice's Reciprocity" and "Sally's Reciprocity (Digital Content Marketplace)".

Although we have assumed the existence of a reputation management system in our hypothetical scenario, there is no evidence, both from the hypothetical scenario and from our analysis in Figure 4-8 that the Escrow Services transmission mechanism handles reputation information internally. The fundamental messages that go into the reputation portion of our analysis in Figure 4-8 (steps 1b(i), 1b(ii) and 5b) exist as a result of the existence of our assumed reputation system. Therefore we conclude that the Escrow Services transmission mechanism does not manage reputation information internally.

There is also no evidence, both from our series of events and from our analysis in Figure 4-8 that the Escrow Services system manages trust information internally, as there is no functionality in the system that provides trust information for Alice concluding or suggesting whether Bob is trustworthy or otherwise.

4.2.3.3 In Depth Analysis

Although we conclude in our analysis that the Escrow Services System does not manage reputation internally, we note that some of the information produced within the escrow server can be used by processes (external to the escrow services transmission mechanism) to facilitate external management of reputation information. For example, the comparison result of the hashes ($H_A(E_K(C))$ and $H_B(E_K(C))$) and descriptions ($D_A(C)$ and $D_B(C)$) in step 3c can be used in a reputation system to indicate Bob's reputation as a trader who consistently delivers the right content to his buyers. If the reputation system records reputation information about Alice as well, then the verification result of Alice's payment $Pay_A(C)$ in step 4a(i)/4a(ii) can be used to indicate Alice's reputation as a buyer who honours her transactions.

From our analysis in Figure 4-8 we note that Alice goes through the trust cycle once completely, starting from "Alice's Reciprocity" in step 1a, going to "Bob's Reputation" in step 1b(ii), then to "Alice's Trust" in step 1c, then going back to "Alice's Reciprocity" in steps 2, 3, 4 and 5a, and finally Alice finishes her trust cycle at "Bob's Reputation" in step 5b.

We note that Bob does not go through the trust cycle with respect to Alice completely at all. Although he starts off at "Bob's Trust" in step 0a, the remainder of his processes are at "Bob's Reciprocity" (for steps 0b, 0c, 2a, 2b and 2c). Unlike Alice, Bob does not go through the "Alice's Reputation" portion of his trust cycle, thus he is unable to obtain or contribute reputation information about Alice into the system. One possible reason for this is the fact that the Escrow Services transmission mechanism relieves Bob from the task of payment verification (as the escrow server performs the operation on Bob's behalf), as a result Bob does not have much significant personal experience with Alice that he may find worthwhile reporting to the reputation management mechanism.

While Bob does not have much information to report to the reputation management mechanism, the same may also be said about Alice. As the Escrow Services transmission mechanism relieves Alice from the task of content verification (checking what Bob promises to deliver with what Bob actually delivers to Alice), information about Bob's reciprocity would have less significance to the other users of the digital content marketplace in deciding to reciprocate with Bob. The type of information in such a trading system that might be of significance to report to the reputation management mechanism would be the quality of Bob's digital content, which is at times difficult to describe with the descriptions $D_A(C)$ and $D_B(C)$ alone.

Considering the Escrow Services transmission mechanism alone (that is, we do not take into account the reputation system and the digital content marketplace as stated in our assumptions in Section 4.2.3.1), we conclude that the Escrow Services System does not facilitate the development of interpersonal trust. We also conclude that the Trusted Third Party nature of the escrow server enables the lowering of trust requirements for Alice and Bob to reciprocate with each other.

Although we conclude that the Escrow Services system does not facilitate the development of interpersonal trust, the fact that the Escrow Services system places itself as a Trusted Third Party for Alice and Bob implies that some form of institutional trust is in place in order for Alice and Bob to participate in the system.

We therefore present our analysis of the Escrow Services system with respect to institutional trust.

From the grey messages in Figure 4-8 of our analysis, we assert that after Bob and Alice reciprocate with each other they evaluate the quality of service provided by the Escrow Server in addition to evaluating the reciprocation with each other. The result of Alice and Bob's evaluations about the Escrow Server affects its reputation as a Trusted Third Party with quality services. Thus we model those evaluation messages as grey messages going from "Alice's Reciprocity" and "Bob's Reciprocity" to "Sally's Reputation". We envisage that the management of Escrow Server's reputation is done informally through "word of mouth" messages. Such "word of mouth" messages may exist in the form of a verbal conversation, message in public forums, or posts in private bulletin boards.

Potential users of the Escrow Services system learn about the system from existing users, and the feedback the users (both existing and potential) obtain from the existing users about the Escrow Services system serve as a form of reputation report about the Escrow Services system. Thus we model the receipt of reputation reports by the buyers and sellers (both potential and existing) of the Escrow Services system in Figure 4-8 as grey messages going from "Sally's Reputation" to "Alice's Trust" and "Bob's Trust" respectively.

After evaluating the feedbacks from the existing users about the Escrow Services system, the potential users decide to participate in the system, and the existing users decide to continue participating in the system. Thus in Figure 4-8 we model these decision messages by the buyers as grey messages going from "Alice's Trust" to "Alice's Reciprocity", and the decision messages by the sellers as grey messages going from "Bob's Trust" to "Bob's Reciprocity".

From our analysis of the grey messages in Figure 4-8 we note that both Alice and Bob go through the trust cycle once completely. Thus Alice's and Bob's trust in Sally develops as they revisit the trust cycles through repeated participation in the Escrow Services System. From the analysis above we conclude that the Escrow Services System facilitates the development of institutional trust between the users of the system and the system itself.

5 Conclusions

It's getting close to the end of the thesis and we know our readers are getting tired and bored with all the mumbo-jumbo we have thrown at them. Do not worry, it's almost over.

The main focus of this thesis is the development of a qualitative, dynamic trust model that can be used in two ways, to analyse various online trading systems for information management mechanisms and to determine whether those systems facilitate the development of trust relationships. We have presented working definitions for the fundamental terms (such as *Trust*, *Reputation* and *Reciprocity*) used in our trust model. We have presented our generic Entity-Interaction model, and our generic trust model for analysing message flows in an online trading system. Our models allow us to analyse message flow among entities in an online trading system, revealing the mechanisms that handle or manage trust, reputation and reciprocity information. We have presented our analysis of three online trading systems, proposed or currently available, using the generic Entity-Interaction model and the generic trust model that we have developed.

The remainder of this chapter is split into three sections. Firstly we critically evaluate our generic trust model highlighting what we see as *the good, the bad and the ugly*. Secondly we summarize our conclusions about the systems that we have analyzed, describing the trust relationships they facilitate as well as their management of information about these relationships. Lastly we comment on some of the future direction that can be taken from this point onwards.

5.1 Our Generic Trust Model

One of our long term contributions in this thesis is the development, refinement and validation of a generic trust model. In Chapter 3 we presented our development of our generic trust model – from our initial considerations of what should and should not be incorporated into our trust model, the actual development of our generic trust model using Mui et al's [Mui 2002] qualitative trust model as our foundation, to the refinement of our trust model by putting it through a generic protocol for developing trust.

We validated our generic trust model by using it to conduct analyses of three online trading systems. From our analysis in Chapter 4 we conclude that our generic

trust model can indeed model the messages that exist in an online trading system, and that the modelled messages flow in the direction of the model arcs (for example, an outgoing message from “Bob’s Trust” always goes to “Bob’s Reciprocity”).

We also conclude from our analysis in Chapter 4 that our generic trust model can facilitate qualitative analysis of the types of trust (for example, interpersonal trust, institutional trust and the like) that is being facilitated by a particular online trading system.

However, we do not claim to have developed a “perfect” model, and indeed we have identified two significant weaknesses. Firstly the effectiveness of the analysis by our generic trust model depends heavily on the quality of the series of events that is constructed for a particular system. We found it necessary to spend a lot of time developing a series of events with enough steps to be useful for modelling and analysis, yet not cluttered with unrevealing “maintenance messages”.

Secondly our generic trust model has difficulties in modelling alternative or branching steps. From the standpoint of our analyses, the ideal message flow is a single-threaded “journey” through our model. However there are many branch points and alternative message flows in the systems we analysed, notably in eBay (see Section 4.2.1.1) and the Escrow Services System (see Section 4.2.3.1). When constructing the message flows for our analyses of these systems from their descriptions and online documentation, we found it difficult to select a representative (“most common” or “most important”) set of messages from these alternatives. One resolution of this problem might be to drive the modelling from the most commonly observed message sequences in an implemented system; however this would mean that our model could only be applied to analyse systems that have been fully implemented (or at least fully simulated). Alternatively, someone might try to develop a more powerful model in which such alternative and branching flows are handled in an elegant manner.

5.2 Summary Descriptions of the Systems

The three online trading systems that we conducted our analysis on are either proposed or currently available. We hereby present the summary descriptions of those online trading systems (see Sections 4.2.1, 4.2.2 and 4.2.3 for detailed descriptions of the systems).

Our first online trading system, eBay, is a prototypical online auction system. It manages the searching and running of auctions created by its users, and provides a "trader feedback" system in which its users may enquire about the feedback on other users.

Our second online trading system, Kazaa, is a popular peer-to-peer file sharing network. The Kazaa application itself manages its users' search queries and file transfers. It also has an "Integrity Rating" functionality that gives files in the Kazaa network a rating. Each rating is assigned by the owner of the file.

Our third trading system, the Escrow Services system, is a proposed peer trading system for digital content. The system ensures that the buyer of the digital content receives what he expects to received from the seller, and that the seller receives his payment from the buyer. The authors of the proposed system focus primarily on the transmission mechanism for the payment and the goods.

5.3 Summary of our Analysis

One of our short-term contributions in this thesis is our analyses of the three online trading systems for the type(s) of trust being facilitated and for their mechanisms for handling and managing trust, reputation and reciprocity information. We present our summary of the analyses as illustrated in Table 5-1 (see Sections 4.2.1, 4.2.2 and 4.2.3 for our detailed analyses of the systems).

	eBay	Kazaa	Escrow Services System
Type of Trust being facilitated	Interpersonal	Institutional	Institutional
Manages Reciprocity Information?	Yes, Internal	Yes, Internal	Yes, Internal
Manages Reputation Information (with respect to the type of trust being facilitated)?	Yes, Internal	Yes, Internal and External	No
Manages Trust Information (with respect to the type of trust being facilitated)?	Yes, External	Yes, External	No
Message flow conforms to our generic trust model?	Yes	Yes	Yes

Table 5-1 Summary of our analyses of the three online trading systems

We note that none of these three online trading systems handle or manage trust information internally, and that two of the three online trading systems we have

analysed manage trust information externally. One possible explanation for the lack of internal management and reliance of external management of trust information by these systems is that they are only designed to *assist* their users in making trust decisions – they are not designed to make those decisions *on behalf* of their users.

We were surprised to discover that all three online trading systems manage reciprocity information internally. However, the fact that they are all *trading systems* of some sort (that is, they are all reciprocity systems) suggests that this observation would be "obvious" to anyone who understands the interplay of trust, reciprocity and reputation in the model of Mui et al [Mui 2002].

Our third observation is that we found only one system which does not rely on some external management of reputation information. This system facilitates interpersonal trust; the other two systems manage institutional trust (one manages reputation information both internally and externally, and the other does not manage reputation information at all). We tentatively conclude that reputation information in institutional trust is primarily managed through external mechanisms such as "word of mouth", advertising, and branding. We note that some of those external mechanisms are same ones that provide the initial trust level for systems trust (see Section 2.2.3 of our Literature Review for details).

Our fourth observation is that the flow of events of the three online trading systems and our subsequent modelled message flows conform to the expected message flows in our generic trust model (for example, a message to "Alice's Reciprocity" always triggers a message from "Alice's Reciprocity" to "Bob's Reputation"). We assert that this lack of an observed contradiction to our model, in dozens of messages in three different systems, is a strong validation of the correctness and predictive power of our model.

5.4 Future Directions

One possible future direction beyond this thesis is to use our generic model to conduct analysis on other online trading systems that are being proposed or currently available. One of such systems is Clark Thomboron's 3D-P2P system [Thomborson 2002] which is proposed for the trading of 3D digital objects among peers.

As we have experienced difficulties in modelling alternative or branching flows with our generic trust model (see Section 5.1 for our discussion of this issue), we advise future users of our generic trust model to apply the "Occam's Razor"

principle when modelling the events in a particular online trading system – that is, we suggest they focus on the modelling of what seems to be the main flow of events in the system, modelling the branching or alternative flows only when this is proved to be necessary.

Another possible future direction is to categorise the messages of various online trading systems using our generic trust model, and using these findings to investigate similarities and differences among system protocols.

We foresee that our generic trust model might help with the protocol design of trust management systems in the future. Our generic trust model provides a framework for system designers during the initial system design, and can also help with the validating and debugging of system protocols.

We also foresee that our generic trust model and our analyses of the existing online trading systems might help users in understanding the inner workings of trust relationship development in an online trading environment, thus they can make better or informed choices in deciding whether to participate in a particular trading network in the future.

Another possible future direction is to develop other trust models from the foundations of our generic trust model. Such trust models may be qualitative or quantitative in nature.

Our last foreseeable and possible future direction beyond this thesis is an obvious one, and it happens to most other theses: being shelved in the university library, only to be to taken out on short loan by some ambitious postgraduate student in the future for his/her literature review.

6 Appendix

6.1 Modelling of Message Flows in Our Generic Protocol

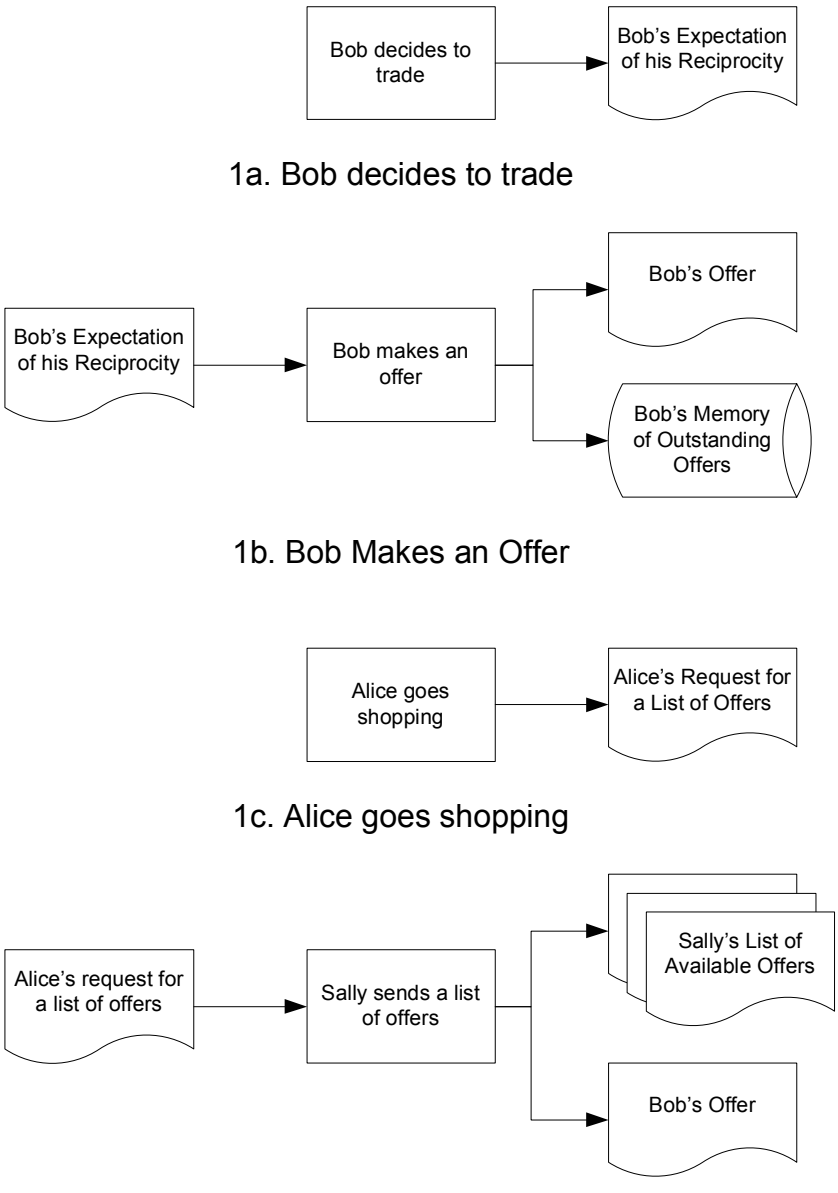


Figure 6-1 Diagram illustrating the interactions among various components in our generic trust model (steps 1a – 1d)

- In step 1a, "Bob decides to trade." (See our complete description of this step in our hypothetical scenario at page 51.) We envisage that after Bob makes his decision to reciprocate he will have some level of expectation about the outcome of his reciprocity in the online trading

system. Thus we label this step's process component with Bob's decision to reciprocate, which results in an outgoing message conveying his expectation.

- In step 1b, "Bob makes an offer." We envisage that the actual offer-making happens as a result of his earlier decision to reciprocate in the online trading system, and that Bob keeps a record of his outstanding offers. Thus the offer-making process is a process component, taking the expectation message from step 1a as the input. We model the actual offer as an outgoing message component, and Bob's record of outstanding offers is a data-store component, which gets updated when Bob makes his offer available in the online trading system.
- In step 1c, "Alice goes shopping." We envisage that Alice's browsing involves sending a message to Sally's online trading system requesting a list of available offers. Thus the browsing process is a process component. Alice's browsing process produces a request for Sally's online trading system to produce a list of available offers, which we model as an outgoing message component.
- In step 1d, "Sally sends a list of offers." We envisage that in addition to Bob's Offer Sally's online trading system will send other offers for Alice to evaluate. Thus the process of sending offers is a process component, taking Alice's request for a list of offers message from step 1c as input. The sending process produces a list of available offers as a series of outgoing message components, along with it is Bob's Offer message (which we have emphasised by separating it from Sally's List of Available Offers message).

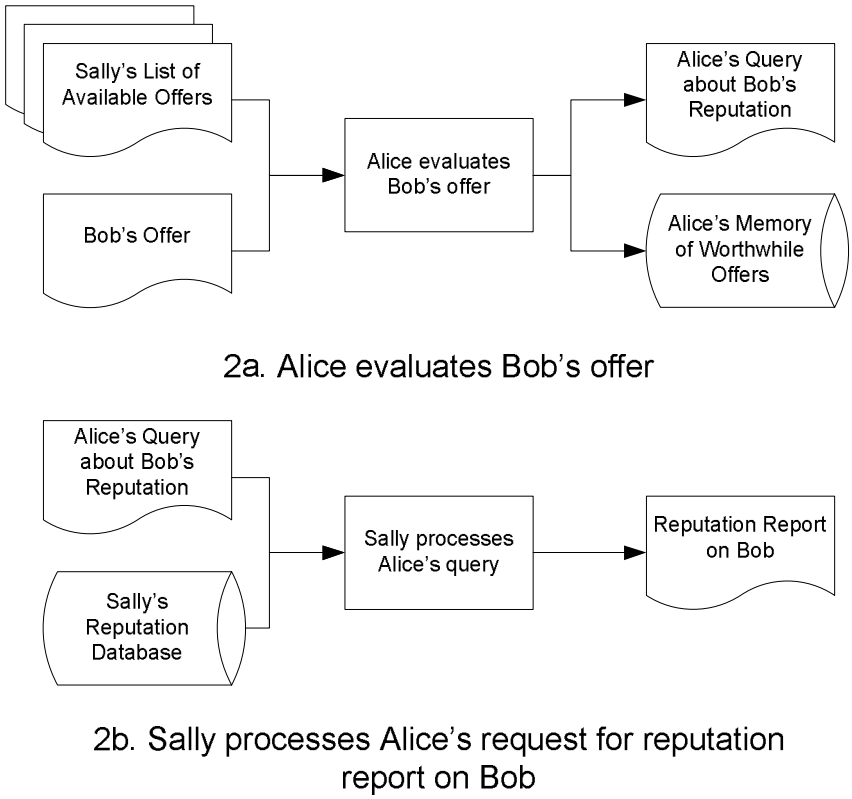
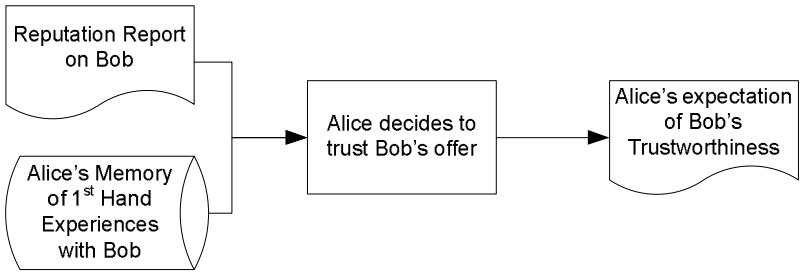
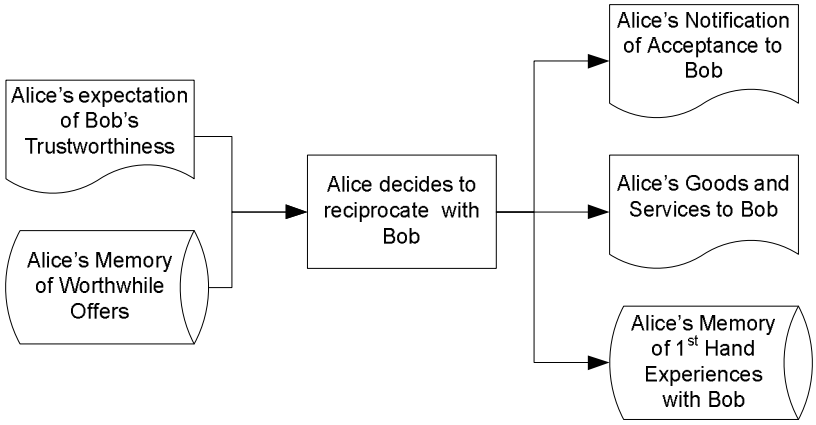


Figure 6-2 Diagram illustrating the interactions among various components in our generic trust model (steps 2a – 2b)

- In step 2a, "Alice evaluates Bob's offer" We envisage that Alice keeps a record of offers that are worthwhile to her. Thus the offer evaluation process is a process component. Alice's evaluation process takes the Sally's List of Available Offers message and Bob's Offer message from step 1d as inputs, and produces a query for Sally to enquire about Bob's reputation, which we model as an outgoing message component. We model Alice's record of worthwhile offers as a data-store component, which gets updated by Alice's evaluation process.
- In step 2b, "Sally processes Alice's query" We envisage that Sally has a reputation database of some sort where she can extract reputation information about Bob from. Thus the query process is a process component, taking Alice's query from step 2a as an input. We model the reputation report as an outgoing message component. We model Sally's reputation database as a data-store component, which is used by the query process to extract reputation information about Bob.



2c. Alice's decision on Bob's trustworthiness

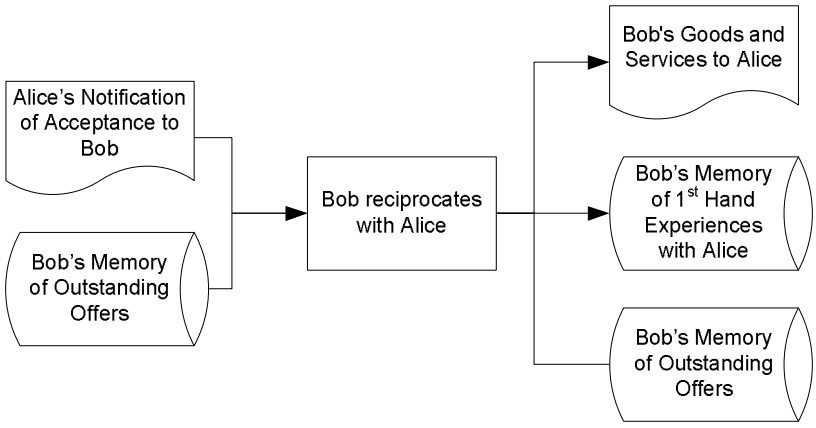


2d. Alice's decision to reciprocate with Bob

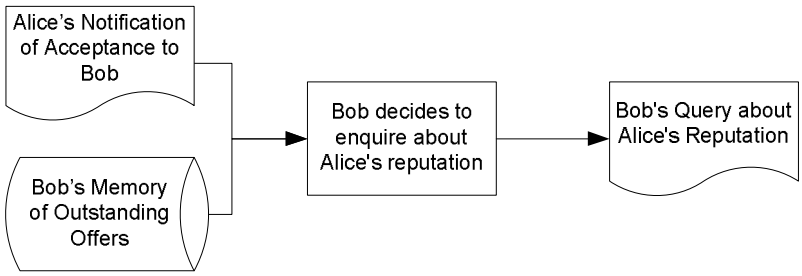
Figure 6-3 2 Diagram illustrating the interactions among various components in our generic trust model (steps 2c – 2d)

- In step 2c, "Alice decides to trust Bob's offer" We envisage that in addition to the reputation report Alice will also enquire into her firsthand experiences with Bob in determining Bob's trustworthiness as a trader (Alice might not trust Bob regardless of what the reputation report asserts about Bob's reputation if she has had bad experiences with Bob). We also envisage that if Alice decides to trust Bob she will have some level of expectation about Bob's trustworthiness. Thus we model Alice's firsthand experiences with Bob as a data-store component, which information within the data-store is to be used in Alice's decision to trust Bob. We label the main processes component in this step with Alice's decision to trust Bob's offer, taking Sally's reputation report message from step 2b and information from Alice's firsthand experiences data-store as inputs, and producing Alice's expectation in Bob's trustworthiness as an outgoing message component.

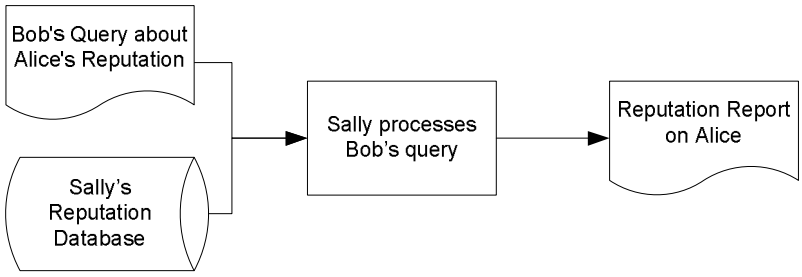
- In step 2d, “Alice decides to reciprocate with Bob” We envisage that Alice will re-enquire her record of worthwhile orders in her decision to reciprocate with Bob. We also envisage that as a result of Alice’s decision to reciprocate with Bob she will have some new personal experiences with Bob. Thus this reciprocity-decision process is a process component, taking the trust-expectation message from 2c and information from her data-store of worthwhile offers as inputs. We model both Alice’s notification of acceptance to Bob and her goods and services as outgoing message components produced by Alice’s reciprocity-decision process. The third output that reciprocity-decision process produces is an update to the data-store of Alice’s firsthand experiences with Bob.



3a. Bob reciprocates with Alice (without consideration of Alice's Reputation)



3b(i). Bob's decision to enquire about Alice's Reputation



3b(ii). Sally processes Bob's request for reputation report on Alice

Figure 6-4 Diagram illustrating the interactions among various components in our generic trust model (steps 3a - 3b(ii))

- In step 3, "Bob reciprocates with Alice" We envisage that Bob will recheck his record of outstanding offers before reciprocating with Alice (as Bob might receive other acceptance notifications to his offer before receiving Alice's acceptance notification), and will update this record when he reciprocates with Alice. We also envisage that through

the reciprocation Bob will have new firsthand experiences with Alice, and that Bob will update his memory of outstanding offers when he reciprocates with Alice (since the offer is no longer "outstanding" when it has been accepted). Thus Bob's reciprocation is a process component, taking Alice's acceptance notification message from step 2c and information from Bob's data-store of outstanding offers as inputs. We model Bob's goods and services to Alice as an outgoing message component produced by the reciprocation process. We model Bob's firsthand experiences with Alice as a data-store component, which gets updated with the latest reciprocation experiences by the reciprocation process component. We also model Bob's data-store of outstanding offers as being updated by the reciprocation process component.

- In step 3b(i), "Bob decides to enquire about Alice's reputation" We envisage that Bob will recheck his record of outstanding offers before deciding to enquire about Alice's reputation. Thus Bob's decision to enquire about Alice's reputation is a process component, taking Alice's acceptance notification message from step 2c, and information from his data-store of outstanding offers as inputs, and producing query to Sally about Alice's reputation as an outgoing message component.
- In step 3b(ii), "Sally processes Bob's query" We envisage that Sally maintains a database storing reputation information. Thus the query process is a process component, taking Bob's query from step 3b(i) and information from Sally's reputation database as inputs, and producing a reputation report about Alice as an outgoing message component.

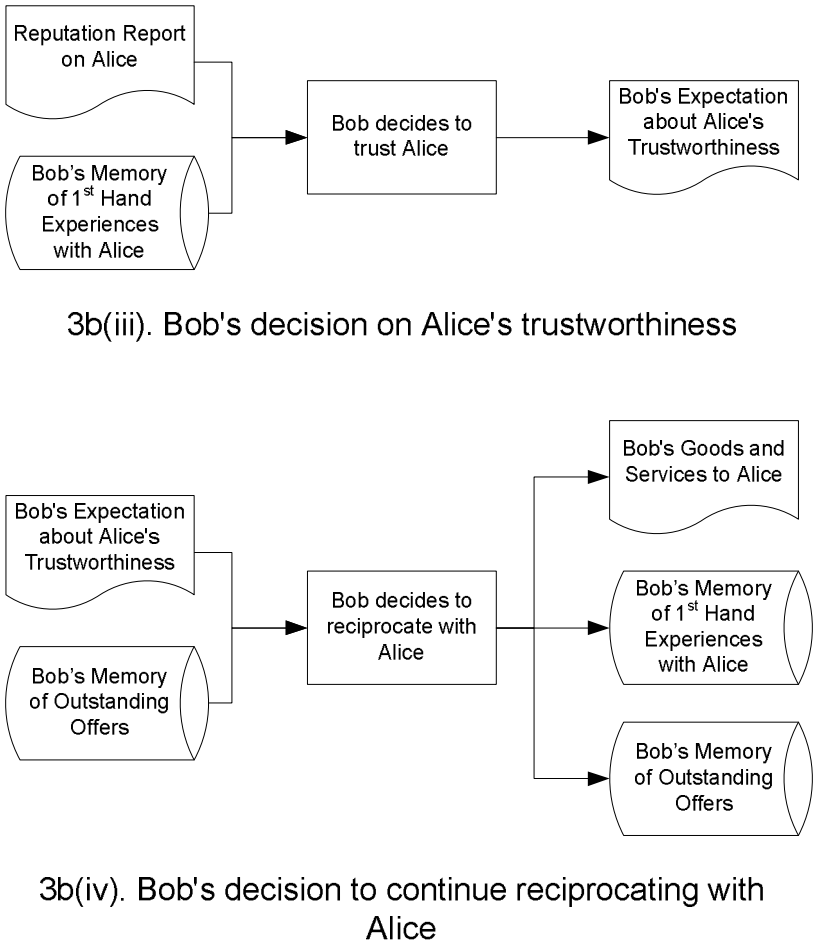
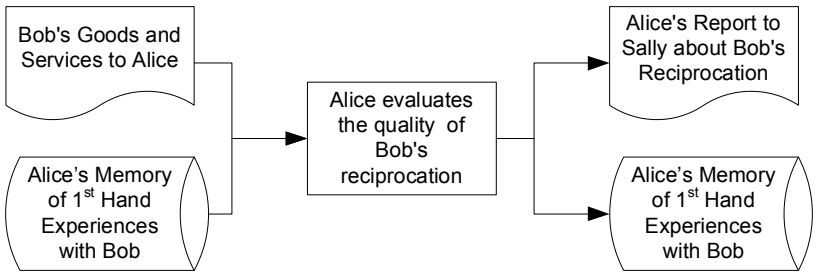


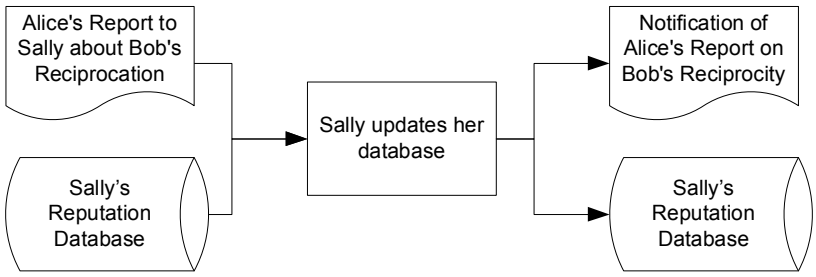
Figure 6-5 Diagram illustrating the interactions among various components in our generic trust model (steps 3b(iii) - 3b(iv))

- In step 3b(iii), "Bob decides to trust Alice" We envisage that in addition to Sally's reputation report Bob will also enquire into his own firsthand experiences with Alice for information. We also envisage that by deciding to trust Alice Bob will have developed some level of expectation about Alice's trustworthiness. Thus we label the main process component in this step with Bob's decision to trust Alice, taking Sally' reputation report message from step 3b(ii) and information from Bob's data-store of firsthand experiences with Alice as inputs, and produces an expectation on Alice's trustworthiness as an outgoing message component.
- In step 3b(iv), "Bob decides to reciprocate with Alice" We envisage that Bob will re-check his memory of outstanding offers before actually delivering his goods and services (as other people might have notified Bob of their acceptance of his offer before Alice does). We

also envisage that Bob will update his memory of outstanding offers, and will have new firsthand experiences with Alice as a result of the reciprocation. Thus the reciprocity-decision process is a process component, taking Bob's expectation of Alice's trustworthiness message and information from Bob's data-store of outstanding offers as inputs. The reciprocity decision process produces Bob's goods and services to Alice as an outgoing message component, and updates new information to Bob's data-store of firsthand experiences with Alice and Bob's data-store of outstanding offers.



4a(i). Alice's evaluation of Bob's reciprocation



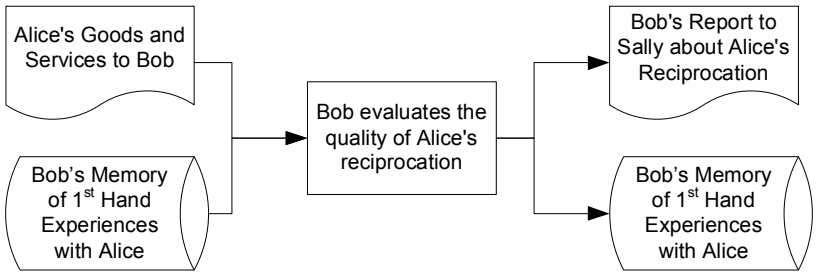
4a(ii). Sally updates Bob's reputation

Figure 6-6 Diagram illustrating the interactions among various components in our generic trust model (steps 4a(i) – 4a(ii))

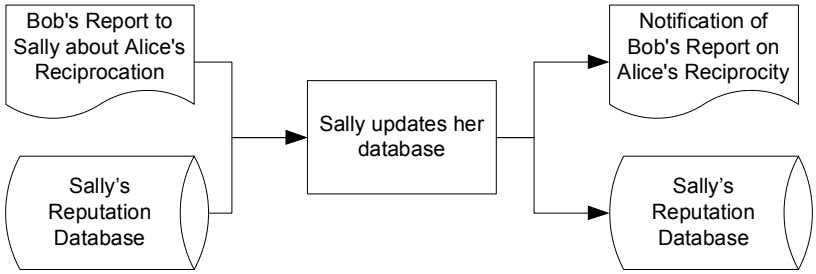
- In step 4a(i), "Alice evaluates the quality of Bob's reciprocation" We envisage that Alice will enquire into her memory of firsthand experiences with Bob in order to compare his previous reciprocations with the current reciprocation. We also envisage that after the evaluation Alice will have new information in her memory of firsthand experiences with Bob. Thus Alice's evaluation is a process component, taking Bob's goods and services message from either step 3a or step

3b(iv) and information from Alice's data-store of firsthand experiences with Bob as inputs. Alice's evaluation process produces Alice's report to Sally about Bob's reciprocity as an outgoing message component, and an update to Alice's data-store of firsthand experiences with Bob.

- In step 4a(ii), "Sally updates her database" we model the database update as a process component, taking Alice's report from step 4a(i) and information from her reputation database as inputs. The update processes produces a notification to Bob as an outgoing message component, produced by the database-update process as an output, and updates Sally's reputation database with information in Alice's report.



4b(i). Bob's evaluation of Alice's reciprocation



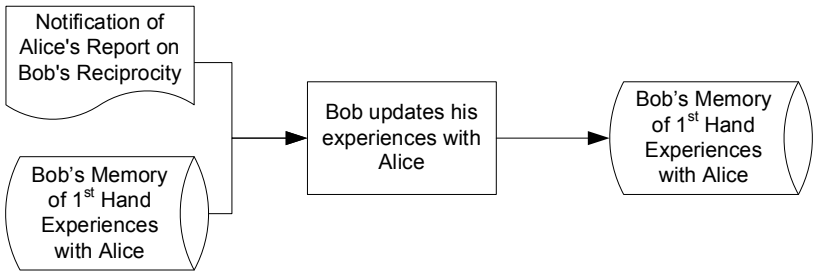
4b(ii). Sally updates Alice's reputation

Figure 6-7 Diagram illustrating the interactions among various components in our generic trust model (steps 4b(i) - 4b(ii))

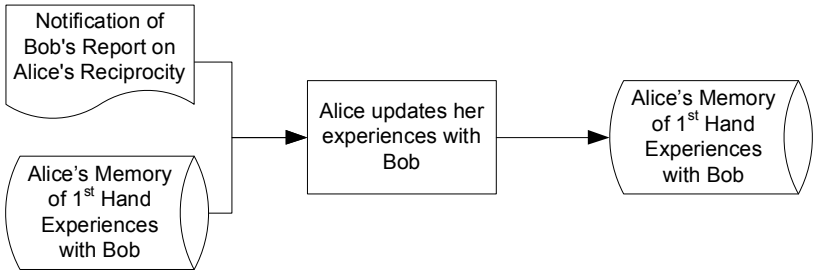
- In step 4b(i), "Bob evaluates the quality of Alice's reciprocation" We envisage that Bob will enquire into his memory of firsthand experiences with Alice for comparisons between the current reciprocation with previous ones (if there is any). We also envisage that Bob will have new firsthand experiences with Alice in his memory. Thus Bob's evaluation is a process component, taking in

Alice's goods and services message from step 2c and information from Bob's data-store of firsthand experiences with Alice as inputs. Bob's evaluation process produces a report to Sally about Alice's reciprocity as an outgoing message component, and an update to Bob's data-store of firsthand experiences with Alice.

- In step 4b(ii), "Sally updates her database" We model the database update as a process component, taking Bob's report form step 4b(i) and information from her reputation database as inputs. The update process updates Sally's reputation database, and produces a notification to Alice as an outgoing message component.



5a. Bob updates his experiences with Alice



5b. Alice updates her experiences with Bob

Figure 6-8 Diagram illustrating the interactions among various components in our generic trust model (steps 5a - 5b)

- In step 5, "Bob updates his experiences with Alice" We envisage that Bob's memory of firsthand experiences with Alice will be updated after reading Alice's report on his reciprocity. Thus Bob's update of firsthand experience is a process component, taking Sally's notification from step 4a(i) and information from Bob's data-store of firsthand

experiences with Alice as inputs, and produces an update to Bob's data-store of firsthand experiences with Alice.

- In step 5b, "Alice updates her experiences with Bob" We envisage that Alice will update her memory of firsthand experiences with Bob after reading Bob's report on her reciprocity. Thus Alice's update to her firsthand experiences is a process component, taking Sally's notification message and information from Alice's data-store of firsthand experiences with Bob as inputs, and produces an update to Alice's data-store of firsthand experiences with Bob.

6.2 Modelling of Message Flows in eBay's Trader Feedback System with respect to the Generic Trust Model

- In Step 1a, Bob decides and offers to engage in a specific reciprocity, namely an auction at eBay. Bob would not do this unless he has sufficient trust in eBay. Thus we model the decision-making message of Step 1a as going from "Bob's Trust" to "Bob's Reciprocity",
- In Step 1b Bob creates an offer and makes the offer available for bidding. Thus we model the auction-creation message as going from "Bob's Reciprocity" to "Sally's Reciprocity (eBay Auction Server)".
- In step 1c Alice goes searching in eBay for possible auctions for her to participate in. Thus we model the search listings message as going from "Alice's Reciprocity" to "Sally's Reciprocity (eBay Auction Server)".
- In step 1d eBay sends Alice a list of open auctions that fits her search criteria. Thus we model this auction listings message as going from "Sally's Reciprocity (eBay Auction Server)" to "Alice's Reciprocity".
- In Step 2a(i), Alice decides to enquire about Bob's reputation after engaging in a reciprocity of browsing through eBay's auction listings. Alice is interested in engaging in a specific reciprocity of trading with Bob through participating in his auction, but she has little knowledge about Bob as to whether he is a trustworthy trader or otherwise. One way of finding out Bob's trustworthiness as a trader is from the feedback left by his previous traders at eBay. That feedback can be aggregated to provide some sort of reputation rating with regard to Bob as a trader. Thus we model the reputation-report-request message of Step 2a(i) as going from "Alice's Reciprocity" to "Bob's Reputation".
- In Step 2a(ii), eBay responds to Alice's request for the reputation report on Bob. The reputation report contains ratings and comments left by traders that Bob has previously traded with. This reputation report is a source of information for Alice in making her trusting choice of engaging with him in a specific reciprocity of participating in

his auction. Thus we model the reputation-report response message in step 2a(ii) as going from “Bob’s Reputation” to “Alice Trust”.

- In Step 2b, Alice decides to trust Bob based on her assessment on Bob’s reputation. Thus we model the trust-decision message in step 2b as going from “Alice’s Trust” to “Alice’s Reciprocity”.
- In Step 2c Alice engages with Bob in a specific reciprocity of participating in his auction through bidding. Thus we model the bidding message as going from “Alice’s Reciprocity” to “Sally’s Reciprocity (eBay Auction Server)”.
- In step 3a(i), eBay notifies Bob that his auction has met the reserve price and sends him Alice’s contact details. Thus we model the notification/contact-details message as going from “Sally’s Reciprocity (eBay Auction Server)” to “Bob’s Reciprocity”.
- In step 3a(ii), eBay notifies Alice that she was the winning bidder in Bob’s auction and sends her Bob’s contact details. Thus we model the notification/contact-details message as going from “Sally’s Reciprocity (eBay Auction Server)” to “Alice’s Reciprocity”.
- In step 3a(iii), eBay updates Alice’s and Bob’s transaction history to include the recent auction. We envisage this step as a database update message to eBay’s databases. Thus we model this database-update message as an internal message within “Sally’s Reciprocity (eBay Auction Server)”. Since the message is an internal message within a component in our generic trust model, it is excluded from Figure 4-3.
- In step 3b(i), eBay notifies Bob that his auction did not meet the reserve price. Thus we model this notification message as going from “Sally’s Reciprocity (eBay Auction Server)” to “Bob’s Reciprocity”.
- In step 3b(ii), eBay notifies Alice that she was the highest bidder for Bob’s auction but the bid did not meet the reserve price. Thus we model this notification message as going from “Sally’s Reciprocity (eBay Auction Server)” to “Alice’s Reciprocity”.
- In step 3c(i), Bob enquires about Alice’s reputation in preparation for the transaction completion stage of his auction. Although Bob is obliged by eBay’s Terms and Conditions to complete the transaction,

he may want to know more about Alice's reputation as a trader before deciding on a strategy (such as the usage of escrow agents) for completing the transaction with her. Thus we model the reputation-report-request message from "Bob's Reciprocity" to "Alice's Reputation".

- In step 3c(ii), eBay responds to Bob of the reputation report about Alice. Similar to step 2a(ii) this reputation report is a source of information for Bob in making his trust-related decision about Alice. Thus we model this reputation-report-response message as going from "Alice's Reputation" to "Bob's Trust".
- In step 3c(iii) Bob evaluates eBay's reputation report about Alice, and based on his evaluation he receives an perception about Alice's trustworthiness, and builds up an expectation of Alice's behaviour in his auction, and decides on a transaction completion strategy. We envisage that Bob will use this transaction completion strategy in his auction which Alice won the bid for. Thus we model this transaction-completion-strategy message as going from "Bob's Trust" to "Bob's Reciprocity".
- In steps 4a(i), Bob contacts Alice to finalise the payment and delivery details of his auction. Thus we model this finalise-transaction-request message as going from "Bob's Reciprocity" to "Alice's Reciprocity".
- In step 4a(ii), Alice replies to Bob with the confirmation of the payment and delivery details for his auction. Thus we model this finalise-transaction-response message as going from "Alice's Reciprocity" to "Bob's Reciprocity".
- In step 4b(i), Alice contacts Bob to finalise the payment and delivery details of his auction. Thus we model this finalise-transaction-request message as going from "Alice's Reciprocity" to "Bob's Reciprocity".
- In step 4b(ii), Bob replies to Alice with the confirmation of the payment and delivery details for his auction. Thus we model this finalise-transaction-response message as going from "Bob's Reciprocity" to "Alice's Reciprocity".

- In steps 4c(i), Bob notifies eBay that he is extending a second chance offer to Alice. Thus we model this second-chance-offer-request message as going from “Bob’s Reciprocity” to “Sally’s Reciprocity (eBay Auction Server)”.
- In step 4c(ii), eBay Auction Server notifies Alice that Bob is extending a second chance offer to her. Thus we model this second-chance-offer-notification message as going from “Sally’s Reciprocity (eBay Auction Server)” to “Alice’s Reciprocity”.
- In step 4c(iii), Alice decides to accept Bob’s second chance offer and notifies eBay of her acceptance. Thus we model this second-chance-offer-acceptance message as going from “Alice’s Reciprocity” to “Sally’s Reciprocity (eBay Auction Server)”.
- In step 4c(iv), eBay notifies Bob that Alice has accepted his second chance offer, and sends him Alice’s contact details. Thus we model this second-chance-offer-acceptance-notification message as going from “Sally’s Reciprocity (eBay Auction Server)” to “Bob’s Reciprocity”.
- In step 4c(v), eBay sends Alice’s Bob’s contact details in response to her acceptance of Bob’s second chance offer. Thus we model this contact-details message as going from “Sally’s Reciprocity (eBay Auction Server)” to “Alice’s Reciprocity”.
- In step 4c(vi), Alice and Bob contact each other to finalise the terms of the transaction (such as payment and delivery details). Depending on the person who initiated the communication one of the [4a(i), 4a(ii)] or [4b(i), 4b(ii)] messaging pairs takes place in this step (The [4a(i), 4a(ii)] pair if Bob initiated the communication, the [4b(i), 4b(ii)] if Alice initiated the communication). Due to the ambiguity of the exact direction of the messages this step has been excluded from our diagram in Figure 4-3.
- In step 4(vii), eBay updates Bob’s and Alice’s transaction history to reflect the changes made from Alice accepting Bob’s second chance offer. We envisage this step as a database update message to eBay’s databases. Thus we model this database-update message as an internal

message within “Sally’s Reciprocity (eBay Auction Server)”. Since the message is an internal message within a component in our generic trust model, its diagramming is excluded from Figure 4-3.

- In steps 5a, Alice sends Bob her payment for his audio system. Thus we model this payment message as going from “Alice’s Reciprocity” to “Bob’s Reciprocity”.
- In step 5b, Bob delivers his audio system to Alice. Thus we model this goods-delivery message as going from “Bob’s Reciprocity” to “Alice’s Reciprocity”.
- In step 6a(i), Alice evaluates her reciprocation with Bob and posts a feedback about Bob at eBay. This feedback is recorded by eBay’s systems and is used in future trader feedback reports on Bob. Thus we model this post-feedback message as going from “Alice’s Reciprocity” to “Bob’s Reputation”.
- In step 6a(ii) eBay sends a notification to Bob about Alice’s recently submitted feedback. This notification may result in Bob reading Alice’s feedback and as a result changes Bob’s expectation on Alice. Thus we model this new-feedback-notification message as going from “Bob’s Reputation” to “Bob’s Trust”.
- In step 6b(i), Bob evaluates his reciprocation with Alice and posts a feedback about her at eBay. This feedback is recorded by eBay’s systems and is used in future trader feedback reports on Alice. Thus we model this post-feedback message as going from “Bob’s Reciprocity” to “Alice’s Reputation”.
- In step 6b(ii) eBay sends a notification to Alice about Bob’s recently submitted feedback. This notification may result in Alice reading Bob’s feedback and as a result changes Alice’s perception on Bob. Thus we model this new-feedback-notification message as going from “Alice’s Reputation” to “Alice’s Trust”.

6.3 Modelling of Message Flows in Kazaa's Integrity Rating System with respect to the Generic Trust Model

- In step 0a, Bob decides to share his files in the Kazaa network. Bob would not do this unless he has sufficient trust in the Kazaa network. Thus we model the decision-making message as going from Bob's Trust to "Bob's Reciprocity".
- In step 0b, Bob applies integrity ratings to the files he is sharing in the Kazaa network. Thus we model the apply-integrity-rating message as one internal to "Bob's Reciprocity" (which is excluded from our diagram in Figure 4-6).
- In step 0c, Bob's Kazaa client submits to his connected supernode the list of files Bob is currently sharing. Thus we model this downloadable-files-list message as going from "Bob's Reciprocity" to "Sally's Reciprocity (Kazaa Supernode)".
- In step 1a(i), Alice submits her search query to her connected supernode. Thus we model this search-query-submit message as going from "Alice's Reciprocity" to "Sally's Reciprocity (Kazaa Supernode)".
- In step 1a(ii), the supernode Alice's Kazaa client is connected to processes Alice's search query, and propagates the search query to other supernodes within the Kazaa network. Thus we model both the process-search-query message and propagate-search-query message as messages internal to "Sally's Reciprocity (Kazaa Supernode)", and thus they are excluded from our diagram in Figure 4-6.
- In step 1a(iii), the supernodes that received Alice's search query propagated by the supernode her Kazaa client is connected to processes the query and submits the results back to the query's originating supernode. Thus we model this propagate-search-query-response message as one internal to "Sally's Reciprocity (Kazaa Supernode)", and thus it is excluded from our diagram in Figure 4-6
- In step 1a(iv) the supernode that Alice's Kazaa client is connected to finishes processing her search query and submits the results back to her

Kazaa client. Thus we model this search-query-results message as going from "Sally's Reciprocity (Kazaa Supernode)" to "Alice's Reciprocity".

- In step 1b(i), Alice instructs her Kazaa client to sort the search results list by integrity rating. In this step Alice is interested in engaging in a specific reciprocity of download a file from Bob (or one of the Bob's), but she has little information about the files besides their metadata. She doesn't know whether the files are of good quality of otherwise. One way of obtaining information about those files is from their integrity ratings left by other user with possession of the file. Those integrity ratings can provide some sort of reputation about the files themselves. Thus we model this sort-search-query-results-request message as going from "Alice's Reciprocity" to Bob's Reputation.
- In step 1b(ii), Alice's Kazaa client sorts the list of search results by integrity rating. The sorted list of search results can be used as a reputation report on the files. This reputation report contains ratings on the files in terms of the relevance of their metadata and content, and the overall quality of the files. Alice uses the information on the reputation report to determine whether she trusts a particular file for its quality. Thus we model this sort-search-query-results-response message as going from Bob's Reputation to Alice's Trust.
- In step 1c, Alice decides to trust that a file with an "excellent" integrity rating is of good quality, and engages in a specific reciprocity of downloading the file onto her computer. Thus we model this decision message as going from Alice's Trust to "Alice's Reciprocity".
- In step 2a, Alice uses her Kazaa client to send file transfer requests to the users with possession of the file she is seeking. Thus we model this file-download-request message as going from "Alice's Reciprocity" to "Bob's Reciprocity".
- In step 2b(i), one of the Bob's Kazaa client which Alice's Kazaa client has sent a file transfer request to decides to accept the file transfer request and proceed with the file transfer. Thus we model this file-

download-request-acceptance message as going from “Bob’s Reciprocity” to “Alice’s Reciprocity”.

- In step 2b(ii), one of the Bob’s Kazaa client which Alice’s Kazaa client has sent a file transfer request to declines her file transfer request. Thus we model this file-download-request-declined message as going from “Bob’s Reciprocity” to “Alice’s Reciprocity”.
- In step 3a, Alice evaluates the quality of the file she has just downloaded using her Kazaa client and provides a rating to the file using her Kazaa client. That rating at this moment is not yet propagated to other users in the Kazaa network. Thus we model this apply-integrity-rating message as one internal to “Alice’s Reciprocity”, and therefore is excluded from our diagram in Figure 4-6.
- In step 3b, Alice’s Kazaa client sends an updated list of downloadable files to its connected supernode. This updated list will contain the new integrity rating that Alice has just given to the files, which will then be propagated to other users in the Kazaa network. Thus we model this downloadable-files-list message as going from “Alice’s Reciprocity” to Bob’s Reputation.

6.4 Modelling of Message Flows in the Escrow Services System with respect to the Generic Trust Model

- In step 0a, Bob decides and offers to engage in a specific reciprocity, namely to sell copies of his digital content *C* in the digital content marketplace. Bob would not do this unless he has sufficient trust in the marketplace. Thus we model the decision-making message as going from "Bob's Trust "to "Bob's Reciprocity".
- In steps 0b, Bob decides on the price *Pr(C)* for which he is selling copies of digital content *C* for, and prepares a description $D_B(C)$, an encrypted version $E_K(C)$ of *C*, and a hash $H_B(E_K(C))$ of the encrypted content. In this step Bob engages in a specific reciprocity of preparing for his sale of his digital content. Thus we model these preparation messages as messages internal within "Bob's Reciprocity", and therefore are excluded from our diagram illustrated in Figure 4-8.
- In step 0c, Bob sends the price *Pr(C)*, the decryption key *K*, the hash $H_B(E_K(C))$ of the encrypted content $E_K(C)$ and the description $D_B(C)$ to the escrow server. Thus we model this new-content-info message as going from "Bob's Reciprocity" to "Sally's Reciprocity (Escrow Server)".
- In step 0d, the escrow server sends a notification to the digital content marketplace about Bob's newly-submitted content. Thus we model this new-content-available message as going from "Sally's Reciprocity (Escrow Server)" to "Sally's Reciprocity (Digital Content Marketplace)".
- In step 1a, Alice browses the digital content marketplace for content worthy of purchasing. In this step Alice engages in a specific reciprocity of browsing the content listings in the digital content marketplace. Thus we model this browse-content-listing message as going from "Alice's Reciprocity" to "Sally's Reciprocity (Digital Content Marketplace)".

- In step 1b(i), Alice decides to enquire about "Bob's Reputation" at the digital content marketplace after engaging in a reciprocity of browsing through the listings at the digital content marketplace. Alice is interested in engaging in a specific reciprocity of trading with Bob through the purchase of his digital content, but she has little knowledge about Bob as to whether he is a trustworthy trader or otherwise, and whether he provides digital content of decent quality or otherwise. One way of finding out Bob's trustworthiness as a trader and as a digital content provider is from the feedback left by his previous traders at the digital content marketplace. That feedback can be aggregated to provide some sort of reputation rating with regard to Bob as a trader and as a digital content provider. Thus we model the reputation-report-request message as going from "Alice's Reciprocity" to "Bob's Reputation".
- In step 1b(ii), the digital content marketplace responds to Alice's request for the reputation report on Bob. The reputation report contains ratings and comments left by traders that Bob has previous sold copies of his digital content to. This reputation report is a source of information for Alice in making her trusting choice of engaging with him in a specific reciprocity of purchase the digital content from him. Thus we model this reputation-report-response message in step 1b(ii) as going from "Bob's Reputation" to "Alice's Trust".
- In step 1c, Alice decides to trust Bob based on her assessment on Bob's reputation, and decides to engage with him in a specific reciprocity of purchasing a copy of his digital content. Thus we model this trust-decision message in step 1c as going from "Alice's Trust" to "Alice's Reciprocity".
- In step 1d Alice contacts Bob with regard to her purchase of Bob's digital content *C*. Thus we model the purchase-digital-content-request message as going from "Alice's Reciprocity" to "Bob's Reciprocity".
- In step 2a(i), Bob contacts Alice with his preferred terms of the transaction. Thus we model this terms-of-transaction message as going from "Bob's Reciprocity" to "Alice's Reciprocity".

- In step 2a(ii), Alice replies to Bob accepting his terms of transaction. Thus we model this term-of-transaction-acceptance message as going from “Alice’s Reciprocity” to “Bob’s Reciprocity”.
- In step 2b(i), Bob advances to Alice a commitment $Com_B(C)$ or the hash $H(C)$ to content C in order to bind Bob to a specific file. Thus we model this commitment-to-digital-content message as going from “Bob’s Reciprocity” to “Alice’s Reciprocity”.
- Nothing happened in step 2b(ii), therefore there are no messages associated with this step, and hence it is not present in our diagram in Figure 4-8.
- In step 2c, Bob sends the encrypted version $E_K(C)$ of the digital content C to Alice. Thus we model this encrypted-digital-content-transfer message as going from “Bob’s Reciprocity” to “Alice’s Reciprocity”.
- In step 3a, Alice computes her hash $H_A(E_K(C))$ for the encrypted content $E_K(C)$. We envisage Alice’s computation as an intermediate step in submitting her payment to the “Sally’s Reciprocity (Escrow Server)”. Thus we model this compute-hash-to-encrypted-content message as one internal to “Alice’s Reciprocity”, and therefore it is not present in our diagram in Figure 4-8.
- In step 3b, Alice sends her hash $H_A(E_K(C))$ of the encrypted content $E_K(C)$, her description $D_A(C)$ of content C, the payment $Pay_A(C)$ for the content and information $ID(B)$ about Bob’s identity to the escrow server. Thus we model this process-payment-request message as going from “Alice’s Reciprocity” to “Sally’s Reciprocity (Escrow Server)”
- In step 3c, the escrow server compares Alice’s hash $H_A(E_K(C))$ of the encrypted content with Bob’s version $H_B(E_K(C))$, Alice’s description $D_A(C)$ with Bob’s description $D_B(C)$ of the content, and Alice’s payment $Pay_A(C)$ with Bob asking price $Pr(C)$. In this step the escrow server engages in a specific reciprocity of comparing various pieces of data submitted from Alice and Bob, which it has the obligation to accomplish. Thus we model these series of comparisons as messages internal to “Sally’s Reciprocity (Escrow Server)”, and therefore they are absent from Figure 4-8.

- In step 3d(i), the escrow server verifies Alice's payment $Pay_A(C)$ after confirming that Bob did send the correct digital content to Alice. In this step the ES engages in a specific reciprocity of verifying Alice's payment, and we envisage that the verification process takes place inside the ES, thus we model this verify-payment message as one internal to "Sally's Reciprocity (Escrow Server)", hence it is absent from our diagram in Figure 4-8.
- In step 3d(ii), the escrow server sends Alice a failure message $Failure(H_A(E_K(C)))$ that her hash $H_A(E_K(C))$ of the encrypted content $E_K(C)$ does not match the hash $H_B(E_K(C))$ originally computed by Bob. Thus we model this hash-comparison-failure message as going from "Sally's Reciprocity (Escrow Server)" to "Alice's Reciprocity".
- In step 4a(i), the escrow server sends Alice a success message $Success(H_A(E_K(C)))$ indicating that her hash $H_A(E_K(C))$ of the encrypted content $E_K(C)$ matches the hash $H_B(E_K(C))$ originally computed by Bob, and sends her the decryption key K to decrypt the digital content. Thus we model this hash-comparison-success message as going from "Sally's Reciprocity (Escrow Server)" to "Alice's Reciprocity".
- No action took place in step 4a(ii), therefore the step is excluded from Figure 4-8.
- In step 4b, the escrow server processes Alice's payment $Pay_A(C)$ and notifies Bob that Alice's payment to him has been processed. We envisage that the processing of Alice's payment takes place inside the escrow server. Thus we model the process-payment-success message sent from the escrow server to Bob as going from "Sally's Reciprocity (Escrow Server)" to "Bob's Reciprocity".
- In step 5a Alice decrypts the encrypted content $E_K(C)$ using the key K sent to her by the ES, and evaluates the digital content C. In this step the decryption of the encrypted content acts as an intermediate step for Alice to engage in a specific reciprocity of evaluating Bob's digital content. Thus we model both the decrypt-encrypted-content message

and evaluate-decrypted-content message as messages internal to "Alice's Reciprocity", and are absent from our diagram in Figure 4-8.

- In step 5b Alice submits her feedback about Bob and/or his digital content to the digital content marketplace. This feedback is recorded by Escrow Services' systems and is used in future trader feedback reports on Bob. Thus we model this post-new-feedback message as going from "Alice's Reciprocity" to "Bob's Reputation".

7 List of References

[Abdul-Rahman 1997] A. Abdul-Rahman and S. Hailes, "A Distributed Trust Model," in Proceedings of ACM New Security Paradigms Workshop, ACM, 1997.

[Abdul-Rahman 2000] A. Abdul-Rahman and S. Hailes, "Supporting Trust in Virtual Communities," in Proceedings of 33rd Hawaii International Conference on System Sciences, IEEE, 2000.

[Aberer 2001] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System," in Proceedings of ACM 10th International Conference on Information and Knowledge Management, ACM, 2001.

[Ahuja 2000] V. Ahuja, "Building Trust in Electronic Commerce," in *IT Professional*, vol. 2, 2000, pp. 61-3.

[Amazon.com 2003] Amazon.com, "Frequently Asked Questions about Reviewers," 2003. [online]. Available: http://www.amazon.com/exec/obidos/subst/community/reviewers-faq.html/104-1273505-7378359 [viewed 25 August 2003]

[Atif 2002] Y. Atif, "Building Trust in E-Commerce," *IEEE Internet Computing*, vol. 6, pp. 18-24, 2002.

[Barber 1983] B. Barber, *The Logic and Limits of Trust*: Rutgers University Press, 1983.

[Barkai 2002] D. Barkai, "Technologies for Sharing and Collaborating on the Net," in Proceedings of First International Conference on Peer-to-Peer Computing, IEEE, 2002.

[BBBOnLine 2003] I. BBBOnLine, "BBBOnline Seal Programs," 2003. [online]. Available: https://www.bbbonline.org/business/ [viewed 26 August 2003]

[Carblanc 2000] A. Carblanc, "Privacy Protection and Redress in the Online Environment: Fostering Effective Alternative Dispute Resolution," in Proceedings of 22nd International Conference on Privacy and Personal Data Protection, 2000.

[Castelfranchi 2000] C. Castelfranchi and R. Pedone, "A Review on Trust in Information Technology," The ALFEBIITE Group, Department of Electrical & Electronic Engineering, Imperial College of Science, Technology & Medicine, UK, 2000. [online]. Available:

http://alfebiite.ee.ic.ac.uk/docs/papers/D1/ab-d1-cas+ped-trust.pdf [viewed 28 August 2003]

[Chen 2001] M. Chen and J. P. Singh, "Computing and Using Reputations for Internet Ratings," in Proceedings of EC' 01, The 3rd ACM Conference on Electronic Commerce, ACM, 2001.

[Cheskin 1999] Cheskin, "eCommerce Trust Study," Cheskin Research and Studio Archetype 1999.

[Cheskin 2000a] Cheskin, "Trust in the Wired Americas," Cheskin Research 2000.

[Cheskin 2000b] Cheskin, "Greater e-China Insights: Online behaviors and attitudes in Greater China," Cheskin Research and chinadotcom Corporation 2000.

[Daignault 2002] M. Daignault, M. Shepherd, S. Marche, and C. Watters, "Enabling Trust Online," in Proceedings of The 3rd International Symposium on Electronic Commerce (ISEC'02), IEEE, 2002.

[Defence 1985] D. o. Defence, "Department of Defence: Trusted Computer System Evaluation Criteria (The Orange Book)," Department of Defence, United States of America, 1985. [online]. Available: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html [viewed 1 September 2003]

[Dellarocas 2000] C. Dellarocas, "Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behaviour," in Proceedings of EC' 00: The 2nd ACM Conference on Electronic Commerce, ACM, 2000.

[Deutsch 1973] M. Deutsch, *The Resolution of Conflict*: New Haven and London: Yale University Press, 1973.

[Dictionary.com 2004] Dictionary.com, "Dictionary.com/entity,"2004. [online]. Available: http://dictionary.reference.com/search?q=entity [viewed 20 January 2004]

[distributed.net 1999] distributed.net, "distributed.net: Project DES," distributed.net, 1999. [online]. Available: http://www.distributed.net/des/ [viewed 26 August 2003]

[eBay 2004a] eBay, "Learn More about Feedback, Your eBay Reputation,"2004. [online]. Available: http://pages.ebay.com/help/feedback/feedback-overview.html [viewed 20 January 2004]

[eBay 2004b] eBay, "How do I sell an item?,"2004. [online]. Available: http://pages.ebay.com/help/welcome/questions/sell-item.html [viewed 20 January 2004]

[eBay 2004c] eBay, "How do I buy an item?,"2004. [online]. Available: http://pages.ebay.com/help/welcome/questions/buy-item.html [viewed 20 January 2004]

[Fung 1999] R. Fung and M. Lee, "EC-Trust (Trust in Electronic Commerce): Exploring the Antecendent Factors," in Proceedings of America Conference of Information Systems (AMCIS 1999), Association for Information Systems, 1999.

[Gambetta 1988a] D. Gambetta, *Trust: Making and Breaking Cooperative Relations*: Basil Blackwell, 1988.

[Gambetta 1988b] D. Gambetta, "Can We Trust Trust?," in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta, Ed.: Basil Blackwell, 1988.

[Gollmann 2002] D. S. Gollmann, "Why Trust is Bad for Security," Lecture to The New Zealand Information Security Forum (www.nzisf.org.nz), The Auckland Club, 34 Shortland St, Auckland, 27 November 2002, Host: Lech Janczewski, l.janczewski@auckland.ac.nz.

[Gutmann 2002] P. Gutmann, "PKI: It's Not Dead, Just Resting (extended version)," 2002. [online]. Available: http://www.cs.auckland.ac.nz/~pgut001/pubs/notdead.pdf [viewed 7 July 2003]

[Horne 2001] B. Horne, B. Pinkas, and T. Sander, "Escrow Services and Incentives in Peer-to-Peer Networks," in Proceedings of The 3rd ACM conference on Electronic Commerce, ACM, 2001.

[Houser 2001] D. Houser and J. Wooders, "Reputation in Auctions: Theory, and Evidence from eBay," Department of Economics, University of Arizona, 2001.

[Jøang 1997] A. Jøang, "The Right Type of Trust for Distributed Systems," in Proceedings of ACM Workshop on New Security Paradigms 96, ACM, 1997.

[Kent 2002] S. Kent, "Rethinking PKI: What's Trust Got to Do with It?," in Proceedings of EUROCRYPT 2002: International Conference on the Theory and Applications of Cryptographic Techniques, 2002.

[Kini 1998] A. Kini and J. Choobineh, "Trust in Electronic Commerce: Definition and Theorectical Considerations," in Proceedings of Thirty-First Hawaii International Conference on System Sciences, IEEE, 1998.

[Konrad 1999] K. Konrad, G. Fuchs, and J. Berthel, "Trust and Electronic Commerce - More Than a Technical Problem," in Proceedings of 18th IEEE Symposium on Reliable Distributed Systems, IEEE, 1999.

[Lai 2002] B. Lai, "Trust in Peer-to-Peer Trading Systems," a Postgraduate Project Report, University of Auckland, Auckland, New Zealand 2002.

[Luhmann 1979] N. Luhmann, *Trust and Power*: John Wiley & Sons, 1979.

[Luhmann 1988] N. Luhmann, "Familiarity, Confidence, Trust: Problems and Alternatives," in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta, Ed.: Basil Blackwell, 1988.

[Manchala 2000] D. W. Manchala, "E-Commerce Trust Metrics and Models," *IEEE Internet Computing*, vol. 4, pp. 36-44, 2000.

[Marsh 1994] S. Marsh, "Formalising Trust as a Computational Concept," *PhD. Thesis*, University of Stirling, 1994.

[McCullagh 2000] A. McCullagh and W. Caelli, "E-Commerce: It *Is* a Matter of Trust (Excerpt)," 2000. [online]. Available: http://eon.law.harvard.edu/trusting/mccullough.html [viewed July 2003]

[McKnight 2001] D. H. McKnight and N. L. Chervany, "Conceptualizing Trust: A Topology and E-Commerce Customer Relationships Model," in Proceedings of The 34th Hawaii International Conference on System Sciences, IEEE, 2001.

[McKnight 2003] H. McKnight, C. Kacmar, and V. Choudhury, "Whoops...Did I use the Wrong Concept to Predict E-Commerce Trust? Modeling the Risk-Related Effects of Trust versus Distrust Concepts," in Proceedings of The 36th Hawaii International Conference on System Sciences, IEEE, 2003.

[Mui 2002] L. Mui, M. Mohtashemi, and A. Halberstadt, "A Computational Model of Trust and Reputation," in Proceedings of The 35th Hawaii International Conference on System Sciences, IEEE, 2002.

[Murphy 2002] T. Murphy and A. K. Manjhi, "Anonymous Identity and Trust for Peet-to-Peer Networks," School of Computer Science, Carnegie Mellon University, 2002. [online]. Available: http://www-2.cs.cmu.edu/~tom7/papers/peer.pdf [viewed 2 March 2003]

[NZX 2004a] New Zealand Stock Exchange, "NZX : NZX Brokers," New Zealand Stock Exchange, 2004. [online]. Available: http://www.nzx.com/market_prof/brokers [viewed 22 February 2004]

[NZX 2004b] New Zealand Stock Exchange, "NZX: Real time data," New Zealand Stock Exchange, 2004. [online]. Available: http://www.nzx.com/products/data_products/real_time [viewed 22 February 2004]

[Ostrom 2002] M. A. Ostrom, "Online auctions are the newest place to hawk stolen goods," SiliconValley.com, 2002. [online]. Available: http://www.siliconvalley.com/mld/siliconvalley/3443962.htm [viewed 18 February 2004]

[Oxford 2003] Oxford, "Oxford English Dictionary," Oxford University Press, 2003. [online]. Available: http://dictionary.oed.com/ [viewed 29 August 2003]

[Palme 1997] J. Palme, "Choices in the Implementation of Rating," in Proceedings of The 5th DELOS Workshop on Filtering and Collaborative Filtering, ERCIM, 1997.

[Patton 2001] M. A. Patton and A. Jøang, "Technologies for Trust in E-Commerce," in Proceedings of IFIP working conference on E-Commerce, 2001.

[PayPal 2004] PayPal, "PayPal,"2004. [online]. Available: http://www.paypal.com/ [viewed 20 January 2004]

[Ratnasingham 2000] P. Ratnasingham and K. Kumar, "Trading Partner Trust in Electronic Commerce Participation," in Proceedings of ACM International Conference of Information Systems, ACM, 2000.

[Rempel 1985] J. Rempel, J. Holmes, and M. Zanna, "Trust in Close Relationships," *Journal of Personality and Social Psychology*, vol. 49, pp. 95-112, 1985.

[Resnick 2000] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, "Reputation Systems," in *Communications of the ACM*, vol. 43, 2000, pp. 45-48.

[RSA-Laboratories 1999] RSA-Laboratories, "DES Challenge III," RSA Laboratories, 1999. [online]. Available: http://www.rsasecurity.com/rsalabs/challenges/des3/index.html [viewed 26 August 2003]

[RSA-Security 1997] RSA-Security, "RSA to Launch "DES Challenge II" at Data Security Conference," RSA Security, 1997. [online]. Available:

http://www.rsasecurity.com/company/news/releases/pr.asp?doc_id=729 [viewed 26 August 2003]

[RSA-Security 1998] RSA-Security, "RSA to Launch DES Challenge III Contest at 1999 Data Security Conference," RSA Security, 1998. [online]. Available: http://www.rsasecurity.com/company/news/releases/pr.asp?doc_id=627 [viewed 25 August 2003]

[Shepherd 2001] M. Shepherd, A. Dhonde, and C. Watters, "Building Trust for E-Commerce: Collaborating Label Bureaus," in Proceedings of The 2nd International Symposium on Electronic Commerce (ISEC'01), 2001.

[Shneiderman 2000] B. Shneiderman, "Designing Trust into Online Experiences," in *Communications of the ACM*, vol. 43, 2000, pp. 57-59.

[Siau 2003] K. Siau and Z. Shen, "Building Customer Trust in Mobile Commerce," in *Communications of the ACM*, vol. 46, 2003, pp. 91-94.

[Sorkin 2001] D. E. Sorkin, "Payment Methods for Consumer-to-Consumer Online Transactions," Sorkin.org, 2001. [online]. Available: http://www.sorkin.org/articles/akron.pdf [viewed 18 February 2004]

[Thawte 2004] Thawte, "Web of Trust," 2004. [online]. Available: http://www.thawte.com/html/COMMUNITY/wot/index.html [viewed 20 January 2004]

[Thomborson 2002] C. Thomborson, “System for Secure Peer-to-Peer Sale of Digital Objects”, private disclosure, July 2002.

[TRUSTe 2003] TRUSTe, "TRUSTe Seal Programs," 2003. [online]. Available: http://www.truste.org/programs/index.html [viewed 26 August 2003]

[Verisign 2003] Verisign, "Secure Site Seal Program," 2003. [online]. Available: http://www.verisign.com/seal/secure/ [viewed 26 August 2003]

[Zhao 1996] J. Zhao, "A WWW Service to Embed and Prove Digital Copyright Watermarks," in Proceedings of The European Conference on Multimedia Applications, Services and Techniques, 1996.