

December 1998

# The Design of a Trusted Third Party for Electronic Commerce Transactions

Sulin Ba

*University of Southern California*

Andrew Whinston

*University of Texas at Austin*

Han Zhang

*University of Texas at Austin*

Follow this and additional works at: <http://aisel.aisnet.org/amcis1998>

---

## Recommended Citation

Ba, Sulin; Whinston, Andrew; and Zhang, Han, "The Design of a Trusted Third Party for Electronic Commerce Transactions" (1998).  
*AMCIS 1998 Proceedings*. 93.

<http://aisel.aisnet.org/amcis1998/93>

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 1998 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

# The Design of a Trusted Third Party for Electronic Commerce Transactions

**Sulin Ba**

Marshall School of Business  
University of Southern California

**Andrew B. Whinston**

**Han Zhang**

Center for Research in Electronic Commerce  
The University of Texas at Austin

## Introduction

The capabilities afforded by network technologies have resulted in numerous electronic commerce applications. But major issues remain which pose serious challenges to the growth and wide adoption of electronic commerce, one being the much talked about security concerns on the Internet (Bhimani 1996 and Froomkin 1996). Proponents of electronic commerce argue that security is a technology issue and has been addressed by various technology developments, such as cryptography, firewalls, and digital certificates, which is true to a certain extent. There is, however, another challenge that has not received as much attention in either the popular press or the research community - the quality uncertainty problem that could result in the public's mistrust in products and services offered online (Choi et al. 1997). Being more of a social and economic issue than a technology challenge, the quality uncertainty problem can severely cripple the development of electronic commerce. How can people promote the trust necessary for efficient online exchange of products and services when individuals have short run temptations to cheat?

Unfortunately, the legal system has not yet caught up with the pace in which electronic commerce is growing. In the absence of a legal system that enforces rules and proper conducts in the electronic marketplace, institutions such as certification authorities (CA) have emerged in recent years. They act as trusted third parties to authenticate individuals and business entities, by attesting to some fact about a digital certificate holder. Most research work done so far on certification authorities focuses on the technology aspect and investigates what technology infrastructure is needed for such trusted third parties to work (Froomkin 1996, McConnell and Appel 1996, Biddle 1997). They fail to address the quality uncertainty problem in electronic transactions. An online vendor who has been authenticated as who he claims he is (i.e., he holds a valid digital certificate) can still cheat consumers by selling counterfeit products or products that do not match up the promised quality.

We propose a new design of trusted third parties that builds on the current structure of CAs. By using a game theoretic approach, we illustrate how extralegal institutions such as trusted third parties can help achieve a proper order for doing business online.

## Product Quality in Electronic Transactions

The online market offers abundant amount of product information for consumers. However, under the disguise of information overflow, there is also information scarcity, a phenomenon that affects the market efficiency by creating information asymmetry (Akerlof 1970). In many situations, information asymmetry has significant implications on the operations of markets (Jensen and Meckling 1976, Caillaud 1990, Greenwald, 1990) and creates the product quality uncertainty problem. Due to the existence of asymmetric information, it is difficult for buyers in the electronic market to have a full knowledge of the product quality or vendor reputation prior to purchase. Legal or non-legal protections are needed to protect the interests of the electronic market players and facilitate the market efficiency.

Research in the law community has argued that in situations where legal mechanisms are not complete, extralegal mechanisms such as informal social norms or non-legal institutions can also help people interact to their mutual advantage (Macaulay 1963, Reid 1980, Ellickson 1991, Bernstein 1992). These norms identify the everyday behaviors that call for the informal administration of rewards and punishments.

Certification authorities (CA) such as Visa or VeriSign emerged in recent years attempting to provide a secure transaction environment. However, what is available from the current structure of CAs is not enough to solve the product quality problem. An authenticated vendor can still cheat a consumer by selling counterfeit products. Additional rules are needed for CAs to function properly for market efficiency. In the following section we specify economic designs that a trusted third party should adopt to be an effective extralegal institution for enforcing honest behavior in the online market.

## Trusted Third Parties as the Enforcement System

Suppose that a seller and a buyer are engaged in an online exchange. Each of them can choose to play either Honest or Cheat. Table 1 presents the payoff structure of the Prisoner's Dilemma game, where  $A > B > C > D$ . This gives both sides

an incentive to cheat (Axelrod 1980, Milgrom et al 1990), even though honest behavior maximizes the total payoff of the two players:  $2B > A + D$ .

Obviously, if this transaction is conducted only once, it is to each player's separate advantage to play Cheat, since that play yields a higher payoff regardless of what the other player does. It is, however, worth noting that both players are worse off than if they could somehow agree to play honest because the payoff of both playing honest is  $B$  while the payoff is only  $C$  if both plays cheat.

**Table 1.**

		Buyer	
		Honest	Cheat
Seller	Honest	$B, B$	$D, A$
	Cheat	$A, D$	$C, C$

In the global online market, a cheater could cheat thousands of times without ever facing the cheated a second time. Each individual transaction thus becomes a Prisoner's Dilemma game where it is never to the player's advantage to be honest. We propose the design of an institution, a trusted third party (TTP), that can help re-enforce honest trading by changing the nature of the transaction to a long term game in which each player's reputation is tied to every single transaction. The TTP is built on the current models of certification authorities (CA) but has enriched functionality. The digital certificate issued by the CAs serve not only as an authentication tool, but also as a reputation indicator. Any one who holds a valid digital certificate should be regarded as a reputable player.

If an online vendor sells fake products or products that are of a less quality than have been represented, unless the vendor paid off all the fines awarded to the cheated parties by the CA, the vendor's digital certificate will be revoked by the issuing CA. This will be an indication to any prospective buyers that this vendor doesn't behave honestly.

Now we formalize the online transaction process to illustrate the TTP's role by structuring the events with the following sequence of play:

1. Before any player is engaged in online transactions, he should apply to TTP for a digital certificate.
2. When players begin to do transaction, they ask each other to provide their digital certificate issued by a TTP. Each player then verifies with the TTP the validity of the certificate, at no utility cost.
3. The two players play the Prisoners' Dilemma game and learn the outcome.
4. Either may appeal to the TTP at personal cost  $K > 0$ , but only if he has checked his partner's digital certificate with the TTP.
5. If either party makes an appeal, then the TTP investigates and awards a judgment,  $J$ , to the plaintiff if he has been Honest and his trading partner has cheated; otherwise, no award is made.
6. If a judgment  $J$  is awarded, the defendant may pay it, at cost  $f(J)$ , or he may refuse to pay, at cost zero. The function  $f : \mathcal{R}^+ \rightarrow \mathcal{R}^+$  represents the utility cost of paying a given judgment and is increasing and continuous. In addition,  $f(x) \geq x$ , that is, what the cheater ends up paying is more than what the TTP awards to the plaintiff
7. Any unpaid judgments result in the revocation of the cheating player's certificate by the TTP.

The desired behavior of the players in various contingencies under the TTP system is described in the following TTP System Strategy (TTPSS).

- a. At substage 1, a player verifies a digital certificate with the TTP if he himself has a digital certificate, but not otherwise.
- b. At substage 2, if either player does not have a digital certificate or if either player has failed to verify the digital certificate, then both players play Cheat (which we may interpret as a refusal by the honest trader to trade); otherwise, both play Honest.
- c. At substage 3, if both players verified the digital certificates at substage 1 and exactly one of the two players Cheated at substage 2, then the victim appeals to the TTP.
- d. At substage 4, if a valid appeal was filed, the TTP awards damages of  $J$  to the cheated party.
- e. At substage 5, the defendant pays the judgment  $J$  if and only if he has a valid digital certificate.

*Theorem.* The Trusted Third Party System Strategy is a symmetric sequential equilibrium strategy of the electronic market transaction game if and only if the following inequality holds.

$$(\delta B - C)/(1 - \delta) \geq f(J) \geq \max[(A - B), f(K)]$$

If this condition is satisfied, then the average payoff per period for each player (at the equilibrium) is  $B$ .

The above steps spell out the design of the trusted third party that would provide protection to consumers and vendors alike, in the absence of legal enforcement. That is, if the inequality holds, no players with the TTP in the electronic market would find it advantageous to cheat.

## Limitations and Conclusion

In section 3 we have spelled out the design of a trusted third party that would provide protection to online traders. However, we do realize that our analysis is based on the assumption that the TTP is a fair and honest judge who is able to make accurate judgment. One can argue that TTPs have their own business interests and objectives. A TTP might be corrupt and solicit bribes from players. Or they might accept voluntary bribes from players who have an unpaid judgment but wish to conceal that fact. Consequently, we need a richer model that addresses the problem of dishonest third parties. Our preliminary analysis indicates that we can find an equilibrium strategy where neither bribing is profitable for the traders nor accepting bribes profitable for the

TTP. Of course, as we add richness to the possibilities for cheating, the functions and strategies of the TTP will have to respond in a correspondingly rich way.

In closing, by introducing a trusted third party that not only issues digital certificate, but also punishes cheating behavior, players can obtain information regarding a trading partner's past history, by verifying whether the partner has a valid digital certificate. In this model, rather than being simply an authentication tool, a digital certificate actually represents a player's reputation. Therefore, even though obtaining complete information about a trading partner is almost impossible in the global online market, the trust third party presents an effective alternative in filling the gap.

### *References*

- Akerlof, G. (1970) "The Market for Lemons: Quality Uncertainty and the Market Mechanism." *Quarterly Journal of Economics*. 84.
- Axelrod, R. (1980) "Effective Choice in the Prisoner's Dilemma." *Journal of Conflict Resolution*. 24(1).
- Bernstein, L. (1992) "Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry." 21 *J. Legal Stud.*
- Bhimani, Anish. (1996) "Securing the Commercial Internet." *Communications of the ACM*, Vol. 39, No. 6.
- Biddle, C. B. (1997) "Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure." *San Diego Law Review*. Vol. 33. Jan.
- Caillaud, B. (1990) "Regulation, Competition, and Asymmetric information." *Journal of Economic Theory*. 52(1).
- Choi, S.-Y., D. O. Stahl, and A. B. Whinston (1997) *The Economics of Electronic Commerce*. Macmillan Technical Publishing.
- Ellickson, R. C. (1991) *Order without Law*. Cambridge, Massachusetts: Harvard University Press.
- Froomkin, A. Michael. (1996) "The Essential Role of Trusted Third Parties in Electronic Commerce." 75 *Oregon Law Journal* 49.
- Greenwald, B. C. (1990) "Asymmetric information and the new theory of the firm: financial constraints and risk behavior." *American Economic Review*. May. 80(2).
- Jensen, M. and W. Meckling (1976) "Theory of the Firm: Managerial Behavior, Agency Costs and Capital Structure." *Journal of Financial Economics* 3. p.305-360.
- Macaulay, S. (1963) "Non-Contractual Relations in Business: A Preliminary Study." 28 *American Sociology Review*. 55.
- McConnell, B. and E. Appel (1996) "Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure." White paper. Available from Office of Management and Budget, Interagency working group on cryptography policy. May.
- Milgrom, P. R., D. C. North and B. R. Weingast (1990) "The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs." *Economics and Politics*. Vol. 2. No. 1, March.
- Reid, John Phillip, 1980, *Law for the Elephant: Property and Social Behavior on the Overland Trail*.