2003

The Key to Trust? Signalling Quality in the PKI Market

James Backhouse
London School of Economics and Political Science, james.backhouse@lse.ac.uk

Carol Hsu
City University of Hong Kong, ischsu@is.cityu.edu.hk

John Baptista
London School of Economics and Political Science, j.m.baptista@lse.ac.uk

Jimmy C. Tseng
Rotterdam School of Management, jtseng@fbk.eur.nl

The key to trust? Signalling quality in the PKI market*

James Backhouse
Department of Information Systems
London School of Economics and Political Science
London, Houghton Street, WC2A 2AE
Tel: + 44 (0) 207 9557641
Fax: + 44 (0) 207 9557385
james.backhouse@lse.ac.uk

Carol Hsu
Department of Information Systems
City University of Hong Kong
Hong Kong, 83 Tat Chee Ave, Kowloon
Tel: +852 21942303
Fax: +852 27888694
ischsu@is.cityu.edu.hk

John Baptista
Department of Information Systems
London School of Economics and Political Science
London, Houghton Street, WC2A 2AE
Tel: + 44 (0) 7776306144
j.m.baptista@lse.ac.uk

Jimmy C. Tseng
Department of Decision & Information Sciences
Rotterdam School of Management
The Netherlands, P.O. Box 1738, 3000 DR Rotterdam
Tel: + 31 104082854
Fax: +31 104089010
jtseng@fbk.eur.nl

* *Funding support from grant number L142251004, the ESRC/DTI Management of Information LINK programme is gratefully received*

Abstract

The absence of a platform for secure electronic commerce is widely recognised. Across the globe, a host of Certification Authorities (CAs) have emerged to seize the opportunity for issuing digital certificates that constitute the Public Key Infrastructure (PKI). Yet the take-up of the technology has been bitterly disappointing. The market for digital certificates has failed to reach the critical worldwide mass that was anticipated. Current literature suggests a variety of outstanding technical, legal and policy issues that hinder the adoption of PKI. We argue that another contributing factor in this adverse turn of events is the quality uncertainty surrounding CAs and the certificates they issue. This paper adopts the Lemons principle, an economic theory, to analyse the market situation of quality uncertainty and reviews three countermeasures that remedy this problem: brand names, guarantees and licensing. Applying this economic theory to the PKI market, the paper discusses how these three countermeasures might be used to signal the quality of certificates and hence generate the trust missing between CAs and relying parties in electronic transactions.

Keywords

Information Security, Public Key Infrastructure, Interoperability, Asymmetry of Information, Economics of IS

1. Introduction

The value of economic theories in the study of information systems (IS) has been demonstrated both by IS researchers and economists. In the IS field, for example, such work includes Malone, Yates and Benjamin (1987) on the use of the market and hierarchy model, Ciborra (1993) on the use of transaction cost theory, and Wigand (1997) on the summary of economic approaches to study electronic commerce. In the economics field, Shapiro and Varian (2002) have used economic theory to analyse information goods and their dynamics in markets. More recently, researchers in the IS security area have begun to use economic theory to understand the incentives for moving away from a given IS secure equilibrium (Anderson, 2002). In keeping with this shift in thinking, this paper examines the current disappointing market situation of Public Key Infrastructure (PKI) through the lens of economic theory.

In recent years, PKI has been developed as a key security technology to provide trust in online transactions and communications. However, some argue that technical difficulties (Ellison and Schneier, 2000; Lloyd, Fillingham, Lampard and Orlowski, 2001), legal and regulatory obstacles (Froomkin, 1996) and privacy concerns (Greenleaf and Clarke, 1997) have prevented PKI from reaching the expected level of success and use. In this paper, we take a market approach to examine the underlying economic dynamics in PKI. From an economic perspective we argue that some of the hesitancy in adopting PKI arises from the existence of quality uncertainty in the PKI market. To demonstrate our argument, we apply Akerlof's Lemons principle illustrating the problem of asymmetric information in the PKI market. The implications of information asymmetry for electronic commerce (Bakos, 2001) and electronic marketplaces (Kaufman and Wood, 2000) have not gone unnoticed, and the concept is used increasingly in the design of countermeasures (Lai, Medvinsky and Neuman, 2000; Millen and Wright, 2000).

The paper commences with a description of PKI and its current vicissitudes. Akerlof's economic theory, the Lemons principle, is used in the second section to explain the problem of quality uncertainty resulting from asymmetry of information between buyers and sellers in markets. In the same section, the paper also briefly discusses the three countermeasures proposed by Akerlof. In the fourth section, the paper identifies the existence of a 'Lemons problem' in the PKI market and examines how countermeasures might be adopted to reduce this quality uncertainty.

2. PKI as a trust mechanism in e-commerce

Trust in electronic commerce can be understood in terms of security principles such as authentication, confidentiality, authorisation and non-repudiation (Wilson, 1999). In the world

of written contracts, these principles can be realised through face-to-face encounter, contracts supported by hand-written signatures and by the established legal framework. To foster the growth of e-commerce, both consumers and businesses need to have confidence in the enforceability and confidentiality of any electronic contract or message exchanged. Accordingly, PKI has been developed with the intention of realising these security principles in an electronic environment.

Adams and Lloyd (1999) define PKI as "a pervasive security infrastructure whose services are implemented and delivered using public-key concepts and techniques". Indeed the concept of PKI is nothing new. The use of public key cryptography, also known as asymmetric key cryptography, began back in the late 1970s (Clarke, 2001). In order to resolve the problem of key distribution in symmetric key cryptography, Diffie and Hellam in 1976 proposed the concept of public key cryptography: the use of different keys to encrypt and decrypt a message. After years of development and evolution, this technique was advanced to the point of enabling the creation of digital signatures and digital certificates, core technical components in PKI today.

Public key algorithms provide the mechanisms of digital signatures and message integrity that serve as forensic evidence in electronic transactions (Ford and Baum, 1997). The reliability of the forensic evidence depends on the ability of the CA to bind identities to their public keys in a digital certificate. A public key infrastructure therefore consists of digital certificates issued by CAs and registration authorities to subscribers and relied upon by relying parties. Each PKI domain is based on a certificate policy that "indicates the applicability of a certificate to a particular community and/or class of application with common security requirements" (Chokhani and Ford, 1999). Each CA within a PKI domain may also publish a Certificate Practice Statement (CPS) detailing the practices it employs when issuing certificates. It is through these important documents that CAs "reduce risk in transacting, establish trust among e-trading parties, thus providing the much-needed security for electronic commerce" (Tseng and Backhouse, 2000).

Thus in the PKI model, CAs bear the greatest responsibility for establishing trust in the electronic world between two mutually unfamiliar identities. CAs are responsible for verifying an applicant's identity, issuing the digital certificate and managing the process of certificate revocation. If a CA makes a mistake at any stage of the certificate life cycle, it increases the opportunity for fraud or other malpractice occasioned by the reliance of a certificate. For example, an incident in January 2001 resulted in Versign issuing two code-signing digital certificates to someone posing as a Microsoft employee (Liew, 2001). Verisign was found at fault in its identification procedures. If this mistake had not been discovered in time, the consequences could have been extremely damaging since it affected most desktop software.

With the expansion of electronic commerce, many companies have been setting up as CAs offering the service of certificate issuance to the public. Our research shows that around the world there are currently at least 103 public-facing CAs. However, we maintain that the considerable growth of PKI services within such a short time scale has led to quality uncertainty

in the market. In a typical electronic transaction, trading parties use digital certificates as their means of identification and authentication. In the situation of open e-commerce, a digital certificate offered as a credential by a subscriber may come from any CA within or outside the same PKI domain. In the market place there exist many different PKI domains, each with its own practices for binding an identity to a certificate. As a result of these variances in security procedures, relying parties cannot be completely certain that certificates emanating from an unknown CA can be trusted and hence whether to rely on them.

The role of information and its impact on markets has been a core subject of study within the economics field. From an economic perspective, the situation we describe above, the existence of quality uncertainty in the PKI market, is a classic example of a "Lemons problem" originating in asymmetry of information. The next section explains this concept and some possible countermeasures for addressing it.

3. The Lemons principle

Akerlof (1970) studied markets with informational gaps between buyers and sellers, and developed the "Lemons principle" as a theoretical framework for understanding the dynamics of markets with this characteristic. He argues that in markets where the quality of the goods is not assessed in the same way by buyers and sellers, the bad quality goods and services tend to drive out the good quality ones, and as a consequence lead to market extinction.

Akerlof (1970) explains that although each individual seller knows the real quality of the good, the buyer does not have access to the same information and is not be able to distinguish between good and bad quality goods. Therefore, the buyer measures the quality of the goods from the market as a whole and is led to assume that all goods in the market have the same average quality. Owing to this asymmetry of information, the seller has an incentive to market lower quality goods for the same average price. At the same time, the better quality goods will not be traded in the market because their true value may not be captured. Consequently, the average quality of goods tends to fall, as well as the size of the market. In extreme circumstances, no market will exist at all.

To illustrate this phenomenon, Akerlof uses the example of the used car market in the US. In this market, there are new and used cars and good and bad cars available. However, the sellers have more information about the true quality of the cars than the buyers, which creates asymmetry of information. Because of imperfect information in the market, the price of a given car will be the same, regardless of its quality. Akerlof (1970) further makes a point that the market price will always be the bad car price. As a result, the good quality car owners will not sell their cars because they cannot realise the true value of their cars. The bad cars gradually drive the good cars out of the market and only bad cars will be traded.

The Lemons model may also be used to analyse the cost of dishonesty. In a market where goods are sold both honestly and dishonestly, quality may be represented fairly or misrepresented. The buyer's problem is to identify quality. As in the "Lemons" cars case, the existence in the market of people willing to offer inferior goods tends to drive the market out of existence. Thus, dishonest dealings have a tendency of forcing honest dealings out of the market, to the extent that no market is possible.

To strengthen his argument for the negative impact of information asymmetry on the market, Akerlof (1970) also analyses the situation of symmetry of information, where all parties share good quality information. In this case, a market is possible and all parties are better off for being able to distinguish the good and bad cars

The work of Akerlof has been adopted by several authors as a generic model of market failure caused by quality uncertainty (Bond 1982, Heinkel 1981, Leland 1979). Our research also shows that the concept of market failure owing to quality variability goes as far back as the 16th Century, when Sir Thomas Gresham propounded one of the best known economic laws: "Bad (or over valued) money drives out good (or under valued) money" (Fetter 1932). However, there is a difference of analogy between the two market concepts. In principle, both agree that good money drives out bad money owing to the existence of a unique market price. Nevertheless, in Gresham's Law both buyers and sellers are able to distinguish between good and bad quality, whereas in the Lemons principle they are not.

Countermeasures

Many researchers have suggested ways in which quality uncertainty or information asymmetry in the market may be reduced. One possible solution is through the concept of signalling. Advocates argue that sellers of the product or service should be allowed to issue costly signals of the quality being offered: in a rational equilibrium, prospective buyers could use these signals to discriminate accurately between products of differing quality (Bhattacharya 1979, Bhattacharya 1980, Ross 1977, Spence 1973, Spence 1974, Spence 1977). Campbell and Kracaw (1980) propose another solution: that sellers make side-payments to information producers to acquire the necessary information at a cost, and convey it to the market. Following this line of thinking, Thakor (1982) proposes the idea of the third party. He identifies three parties in the market structure: a group of sellers, each aware of the quality of its own product; a set of buyers who satisfy the rational-expectations assumption that they are aware of the average quality of the products in the market, but are unable to distinguish one seller from the other on the basis of product quality; and "third party" information producers who expend resources to produce information about the quality of each product offered for sale. Thakor (1982) argues that market failure as explained by the Lemons principle can be prevented if a priori imperfectly informed buyers of a given product can somehow revise their initial conditional estimates of product quality.

At a specific level, Akerlof (1970) suggests that market players can implement three types of countermeasures to mitigate the effects of asymmetry of information: guarantees, brand names, and licensing. Guarantees exist to assure the buyer of normal expected quality. Brand names not only serve to indicate quality but also offer a better chance of consumer retaliation should quality not match expectation. Umbrella branding (where new products are associated with older brands) is often used for quality perception extension. Licensing, certification and even education can also reduce quality uncertainty. For example, skilled labour often requires certain licenses and certificates to work and employers also use educational qualifications, such as degrees, to reduce uncertainty about an employee's quality.

This part of paper has briefly identified some countermeasures for overcoming the Lemons problem. The next section applies the Lemons principle in the PKI context. From this analysis it is possible to recognise the existence of quality uncertainty in the PKI market. We also examine how the market is currently using the three countermeasures proposed by Akerlof to combat this problem.

4. Applying the Lemons principle in the PKI market

In the preceding section, Akerlof (1970) considers a general class of situations in which qualitative uncertainty about a product combines with "unravelling effects" on individual behaviour to influence the average quality of the products traded and sometimes the actual existence of the market for the good. The Lemons principle is now applied in the PKI environment. We have chosen the used car market as an analogy for information asymmetry in the PKI market.

In the used car market there are two main parties involved: the car seller and the buyer. In the PKI market, on the one hand, there is the party which accepts (or not) the digital certificate, i.e. the relying party, and on the other hand the issuer of the certificate, i.e. the CA. Trust is required when the relying party has to make a transaction decision based on the credibility of the information provided by the digital certificate.

In Akerlof's example, used cars could be of various grades of quality between good and bad. Likewise, in the PKI market there are certificates with various qualities. As seen in section two, the spread of CAs through out the world, with their different procedures, technologies and legal frameworks has contributed to the existence in the market of certificates with variable quality. In addition we argue that consumers' unfamiliarity with the use of digital certificate for electronic authentication and transactions has further exacerbated the problem of imperfect information. Many certificate users have no technical or legal understanding of how digital certificates really work and what are the associated risks. This creates the incentive for

opportunistic behaviour by CAs to under-invest in technology and operational procedures for the creation of digital certificate, which in turn compromises the quality of the certificate. Following the logic of the "Lemons principle", we maintain that this market exhibits the asymmetry of information regarding the certificate between the CA and the relying party. As a consequence, relying parties are unable to distinguish the quality of a digital certificate and hence assume that all certificates are of average quality. Therefore good quality certificates will be seen and accepted as if they were of average quality. This could lead, after several feedback loops, to only low quality certificates remaining in the market, the bad quality certificate driving out the good.

However, as suggested by Akerlof (1970), the problem of information asymmetry can be circumvented or mitigated. Three different signalling mechanisms can provide credible information about the quality of the digital certificate to the relying party, and as a result, the relying party is able to assess the real quality of the digital certificate and the level of risk associated with its acceptance. Incorporating this new information into a risk management strategy, a relying party can then make an informed decision on whether to accept a particular certificate or not. Without the signalling devices it can be a difficult task to distinguish the quality of the incoming certificate, and the "Lemons" effect may sink the PKI market entirely.

Countermeasures for the Lemons problem in the PKI market

As indicated in section three, Akerlof (1970) suggests three mechanisms for reducing quality uncertainty in the market: guarantees, brand names, and licensing. In the PKI market, we see evidence of these countermeasures already in place. There follows a discussion on how these mechanisms are implemented and what issues remain for further consideration.

On the implementation of guarantees, Akerlof (1970) makes a point that the provision of a guarantee by the seller can offer a degree of assurance for product or service to the buyer. In the PKI market, the disclosure of certification practices is intended to establish confidence in the CA. However, the mechanism used to signal quality is curtailed by statements limiting liability in a CPS. The industry CPS standard RFC2527 recommends that the CA should declare its liability clearly under the section of "Limitation and Warranty". However, our research shows that in reality there is no standard practice regarding the extent of liability of a CA in the event of a security breach or for any other damages caused by the use or reliance on a digital certificate. Furthermore, most CAs set a limit for liability associated with different types of certificates, commercial Certificate Practice Statements. These are crafted to limit the CA's liability. To complicate the problem further, each CA often has its own classification scheme defining the types of certificates and its associated limitations.

There are other concerns regarding this countermeasure. In general, before accepting a digital certificate, a relying party needs to understand the limitations or conditions of liability. Thus for each unknown certificate, relying parties need to go through the exercise of locating the CPS as

well as understanding its content. There are several problems in this process. Firstly, our research shows that not all CPSs are available online. Since the CPS may contain detailed information on its security procedures, some CAs maintain that publishing a CPS increases risk unacceptably. Secondly, there is no guarantee that the language in which the CPS is written is intelligible to the relying party. In the case that the CPS is inscrutable, the relying party has no way of knowing what protection in available from the CA under the terms of the guarantees in the CPS. Finally with no case law yet to establish precedent, it is unclear which laws might apply to digital certificate and how the courts might apply them. Hence until there are precedents it may be difficult to use liability as a sole device for eliminating poor quality certificates in the market.

The second countermeasure in Akerlof's view is the use of brand names. Market research literature has shown that when purchasing a product a brand name is an important element in a consumer's decision-making process (Chu and Chu, 1994; Jacoby, Szybillo and Busato-Schach, 1977). Thus in promoting a new product or service, manufacturers can use brand names as a signal for product quality. In the PKI market, we also detect the adoption of branding as a marketing strategy for attracting potential certificate subscribers. Our research indicates that many CAs in the market have been established either by telecommunication companies or postal service companies. Such companies already have experience in providing trust services, such as passport registration or telephone directories. It would be natural for them to extend their existing services to the electronic environment. Instead of setting up a new company, these organisations are using their existing brand names to advertise their new services. This fits well with what Wernerfelt (1988) described as "umbrella branding" (Wernerfelt, 1988). The practice of umbrella branding is to use the established brand name for promoting new experience goods. Wernerfelt refers to experience goods as products "whose quality cannot be determined by inspection, so that consumers need to buy the product to learn its quality" (Wernerfelt 1988: 458). Further he asserts that only firms with two good quality products would use this branding strategy, otherwise, an old product with bad quality would consequently lead to the loss of both products. In the context of the PKI market, many consumers have already relied on the same telecommunication or postal services for many years, and generally have good faith in their quality. Therefore, when these companies launch a new service such as certification, consumers may tend to assume that the service quality offered by these companies will be better than that of others in the market.

Chain stores can have the same level of impact in the market as brand names. One good example is the dominant position of McDonalds as compared with a local hamburger bar. In the PKI market, we found that the chain store strategy is also alive and prospering for such companies as Verisign or Globalsign. To penetrate the market, as well as to capture a large market share, these companies have seized the first mover advantage by entering the market early and expanded by establishing a network of CAs in different parts of the world. The 'chain store' network is constructed either by strategic alliances or setting up local companies. For instance, our research shows that at present Globalsign already has 6 subsidiaries in the world. From the perspective of the chain store strategy, when consumers face the choice of different CAs, they often choose the one with a global reputation: companies such Versign and Gloalsign will stand out from other CAs. As well as being a multinational brand, the chains strategy can

also be implemented through the game of being "one of the club". However, we recommend that more research is required before a judgement can be made on the effectiveness of the brand name and the chain strategy as signals for certificate service quality.

The third mechanism for signalling product quality is the method of licensing. In the economics field, the notion of imposing minimum quality standards has been applied both to professions and to products. Leland (1979) offers the example of licensing doctors or accountants as well as drugs. Swann and Temple (1996) investigates the effect of standards on trade performance. In their work, they analysed the impact of British standards on exports and imports performance in the UK context. The findings suggest that "UK standards appears to increase UK exports and UK imports, though the effect on exports is stronger than on imports" (Swann et al.,1996 pp.1311). In the IS security field, licensing and minimum quality standards have also been around for a long time. Examples include the Orange Book on security product evaluation, BS7799 on IS security management and CISA on IS security professionals. In the context of PKI market, we discern two broad types of licensing methods: compulsory licensing and voluntary accreditation. The former refers to the situation in which a CA needs to meet certain legal requirements in order to operate in a country or a particular community. The latter refers to the situation in which a CA voluntarily takes up an accreditation scheme. Compulsory schemes are practised in some countries such as those embodied in the Digital Signature Law in Malaysia and the Digital Document Regulations in Italy. In these countries, governments can assure consumers that all CAs meet the minimum quality standard. In the legal terms, this is also known as the technology-specific approach (Kuner et al. 2000; Wilson 2001). Voluntary accreditation can also be offered by government agents or commercial entities. Examples of these schemes include Gatekeeper in Australia, WebTrust in North America and tScheme in the UK. We consider two reasons why a CA might pursue a particular voluntary accreditation scheme. First, a CA might take up a scheme because of business requirements. In the case of Gatekeeper, the government only accepts certificates issued by a Gatekeeper certified CA. In the case of WebTrust, Microsoft now requires that for Root CAs to be included in Microsoft Explorer, they must have succeeded in the WebTrust audit (KPMG 2002). Thus in order to attract certificate subscribers who wish to do business, say, with the Australian government or through Microsoft Explorer, a CA must invest in acquiring voluntary accreditation. Second, a CA might decide to use an accreditation scheme as a device to increase the level of consumer trust in general. For instance, with the seal of approval from tScheme accreditation in the UK, CAs such as Certificate Factory and OnSite can demonstrate their quality service to the public. Nevertheless, there are variances in the evaluation criteria that apply to the existing CA accreditation schemes. In our view more government and industry effort is still needed to ensure the quality standard across different accreditation schemes.

5. Conclusion

In this paper we demonstrate the nature of information asymmetry in the PKI market by using the "Lemons principle". We then examine both the problems of, and possible countermeasures

for, quality uncertainty in the current PKI market. Besides applying the model to analyse the PKI market, we further discuss the current value of three countermeasures for addressing quality uncertainty in the market. In this discussion, we examine how each method is currently implemented in the PKI market and what further problems need to be addressed in order to increase the effectiveness of any such signal. As a result of this discussion, we hope to increase understanding of the barriers holding back adoption of PKI and to offer an economic perspective on a resolution. While we acknowledge the technical difficulties and the legal and policy obstacles addressed within the information security literature, we contend that the problem of information asymmetry is a contributory factor in the slow take-up of digital certificates in the PKI market. Embracing an economic perspective brings additional insight into the mechanisms for enhancing the level of trust and confidence in third-party trusted services and consequently for electronic commerce in general.

References

Adams, C. and Lloyd S. (1999) *Understanding Public Key Infrastructure: Concepts, Standards and Deployment Considerations,* Macmillan Technical Publishing, Indianapolis, USA.

Akerlof, G. (1970) "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism", *Quarterly Journal of Economics,* 89 pp. 488-500.

Anderson, R. (2002) “Economics and Security Resource Page” http://www.cl.cam.ac.uk/~rja14/econsec.html

Bakos, Y (2001) "The Emerging Landscape for Retail E-Commerce." *Journal of Economic Perspectives*, January 2001

Bhattacharya, S. (1979) "Imperfect Information, Dividend Policy, and the "Bird in the Hand Fallacy"", *The Bell Journal of Economics,* 10 pp. 259-270.

Bhattacharya, S. (1980) "Nondissipative Signalling Structures and Dividend Policy", *Quarterly Journal of Economics,* 95 pp. 1-24.

Bond, E. (1982) "A Direct Test of the Lemons Model: The Market for Used Pickups Trucks", *The American Economic Review,* 72 pp. 836-840.

Campbell, T. and Kracaw, W. (1980) "Information Production, Market Signalling and the Theory of Financial Intermediation", *The Journal of Finance,* 35 pp. 863-882.

Chokhani, S. and W. Ford (1999) " Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework", IETF RFC 2527

Chu, W. and Chu, W. (1994) “Signalling Quality by Selling through a Reputable Retailer: An Example of Renting the Reputation of Another Agent”, *Marketing Science*, 13 (2) pp. 177-189

Ciborra, C. (1993) *Teams, Markets and Systems: Business Innovation and Information Technology*, Cambridge University Press, Cambridge UK

Clarke, R. (2001) "The Fundamental Inadequacies of Conventional Public Key Infrastructure". in *Global Co-Operation in the New Millennium,* pp. 148-159, Bled, Slovenia, June 27-29.

Ellison, C. and Schneier, B. (2000) "Ten Risks of PKI: What You Are Not Being Told About Public Key Infrastructure", *Computer Security Journal,* pp.1-8, XVI.

Fetter, F. (1932) "Some Neglected Aspects of Gresham's Law", *The Quarterly Journal of Economics,* 46 pp. 480-495.

Ford, W. and Baum, M. (1997) *Secure Electronic Commerce : Building the Infrastructure for Digital Signatures and Encryption,* Prentice Hall, Upper Saddle River, N.J.

Froomkin, Michael A. (1996) "The Essential Role of Trusted Third Parties in Electronic Commerce", 75 Oregon L. Rev. 49

Greenleaf, G. and Clarke, R (1997) `Privacy Implications of Digital Signatures', IBC Conference on Digital Signatures, Sydney

Heinkel, R. (1981) "Uncertainty Product Quality: The Market for Lemons with an Imperfect Testing Technology", *The Bell Journal of Economics,* 12 pp. 625-636.

Jacoby, J., G. Szybillo and J. Busato-Schach (1977) "Information Acquisition Behaviour in Brand Choice Situations", *The Journal of Consumer Research*, 3 (4) pp. 209-216

Kauffman, Robert J. and Charles A. Wood (2000) "Analysing Competition and Collusion Strategies in Electronic Marketplaces with Information Asymmetry", University of Minnesota Management Information Systems Research Center Working Paper No. 00-19.

KPMG (2002) *Digital Certificates, Authentication and Trust on the Internet*, www.kpmg.nl/irm.

Kuner et al. (2000) "An Analysis of International Electronic and Digital Signature Implementation Initiatives", The Internet Law and Policy Forum

Lai, C., G. Medvinsky, and B. C. Neuman, (1994) "Endorsements, Licensing, and Insurance for Distributed System Services," In Proc. of the 2nd ACM Conf. on Computer and Comm. Security , 170--175, Nov. 1994.

Leland, H. (1979) "Quacks, Lemons and Licensing: A Theory of Minimum Quality Standards", *The Journal of Political Economy,* 87 pp. 1328-1346.

Liew, M. (2001) "Digital Certificate Fraud", Com*puterworld,* 7 (21), 6-12 April.

Lloyd, S., D. Fillingham, R. Lampard and S. Orlowski (2001) "CA-CA Interoperability" *PKI Forum TWG*

Malone, T., J. Yates and R. Benjamin (1987) "Electronic markets and electronic hierarchies" *Communications of the ACM,* 30(6) pp. 484-497

Millen, Jonathan K. and Rebecca N. Wright (2000) "Reasoning about Trust and Insurance in a Public Key Infrastructure" Proceedings of The 13th Computer Security Foundations Workshop, July 03 - 05, 2000, Cambridge, England

Ross, S. (1977) "The Determination of Financial Structure: The Incentive Signalling Approach", *The Bell journal of Economics,* 8 pp. 23-40.

Shapiro, C. and Varian, H. (2002) *Information Rules: A Strategic Guide to the Network Economy,* Harvard Business School Press, Boston.

Spence, M. (1973) "Job Market Signalling", *Quarterly Journal of Economics,* 87 pp. 355-374.

Spence, M. (1974) "Competitive and Optimal Responses to Signals: Analysis of Efficiency and Distribution", *Journal of Economic Theory,* 7 pp. 296-332.

Spence, M. (1977) "Consumer Misperceptions, Product Failure and Producer Liability", *Review of Economic Studies,* 3 pp. 561-572.

Swann, P. and P. Temple (1996) "Standards and Trade Performance: the UK Experience" *The Economic Journal*, 106(438) pp.1297-1313

Tseng, J. and J. Backhouse (2000). "Searching for Meaning-Performatives and Obligations in Public Key Infrastructure". The Fifth International Workshop on the Language-Action Perspective on Communication Modelling, Aachen, Germany.

Thakor, A. (1982) "An Exploration of Competitive Signalling Equilibria with "Third Party" Information Production: The Case of Debt Insurance", *The Journal of Finance,* 37 pp. 717-739.

Wernerfelt, B. (1988) " Umbrella Branding as a Signal of New Product Quality: An Example of Signalling by Posting a Bond", *Rand Journal of Economics*, 19 pp 458-466

Wigand R. (1997) "Electronic Commerce: Definition Theory and Context" *The Information Society*, 13 pp. 1-16.

Wilson, S (1999) "Digital Signatures and the Future of Documentation" *Information Management & Computer Security*, 7(2) pp 83-87

Wilson, S (2001) "A Comparison of Authentication Technologies in E-Business" *The Asia Business Law Review*, July