By James Backhouse, Carol Hsu, Jimmy C. Tseng, *and* John Baptista

A Question of Trust

An economic perspective on quality standards in the certification services market.

Despite nearly a decade of intensive effort by the computer science and legal communities, establishing interoperation of trust services remains one of the key challenges for e-commerce. Many early commentators had high hopes that the advent of Public Key Infrastructure (PKI) would provide the basis for securing electronic transactions and establishing trust. It is now increasingly evident that such early aspirations were overly optimistic and the adoption of PKI has in fact been more limited. There are differing accounts of the sluggish PKI take-up in the market, each focusing on particular issues in PKI, for example security and risk [6], interoperability [9], privacy concerns over identity-based certificates [5], and legal obstacles [11].

While much progress has been made through collaborations between technical and legal experts [7], other information security researchers have begun to turn to economics for further insight into information security [4] and risk management [8]. This article argues, from an economic perspective, that one of the factors contributing to the hesitancy in adopting commercial trusted third-party services pertains to quality uncertainty in the certification services market. We explain the problem of quality uncertainty as resulting from the asymmetry of information between buyers and sellers, and illustrate the existence of such a problem in the certification services market. Further, we review existing implementations of standards as signaling devices for reducing quality uncertainty in the trust services market. Finally, we reflect on the current situation and consider the role of standards in enhancing market effectiveness.

Std Body	Standard	Title	Purpose
ISO/ITU-T	ISO/IEC 9594-8 (1995: ITU-T Rec X.509 v3) (2000: ITU-T Rec X.509 v4)	Information technology—Open Systems Interconnection—The Directory: Public key and attribute certificate frameworks	Standard format for X.509 public key certificates See www.iso.ch
IETF	IETF RFC 3280 (RFC 2459)	X.509 Public Key Infrastructure Certificate and CRL Profile	Proposed standard for public key certificates See www.rfc-editor.org
IETF	IETF RFC 3647 (RFC 2527)	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	Information for authors of certificate policies and certification practice statements (added section 9 on business and legal model)
ETSI	ETSI TS 101 456	Policy requirements for certification authorities issuing qualified certificates	Policy requirements for certification authorities issuing qualified certificates (See also RFC 3237)
American Bar Association	PAG	PKI Assessment Guidelines	CA guidelines from lawyers See www.abanet.org
American Institute of Certified Public Accountants	WebTrust	WebTrust Program for Certification Authorities	CA accreditation guidelines from accountant and auditors See ww.aicpa.org/webtrust or www.cpawebtrust.org/
NACHA Internet Council	CARAT Guidelines	Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates	CA guidelines for the banking sector See internetcouncil.nacha.org/

Table 1. Standards and best-practice guidelines in PKI.

Contractual Relationships in Certification Services

At least three parties are involved in the certification services market. First, there are third-party certification service providers also known as Certification Authorities (CAs), entities that serve as the anchor of trust between two previously unknown (to each other) identities in the electronic world. Second, certificate holders, also known as subscribers, are the persons or organizations subscribing to the certification service of a CA. Third, the other end users of the certification services, also known as relying parties, are those persons or organizations placing reliance on the certificate to authenticate the certificate holder. To establish trust, the various parties are bound together through a series of contractual relationships, through an explicit set of agreements, or otherwise implicitly through the obligations and liabilities commonly enshrined in policy documents such as the certificate policy (CP) and certificate practice statement (CPS) (see the figure here). The former describes the set of rules applicable to a class of certificates, while the latter details the operational practices of the CA. Since the trustworthiness of the certification service providers is only as great as the guarantees and warranties they offer, numerous standards and best-practices guidelines have been advanced to clarify the obligations and liabilities in the business and legal model of a certification service provider (see Table 1).

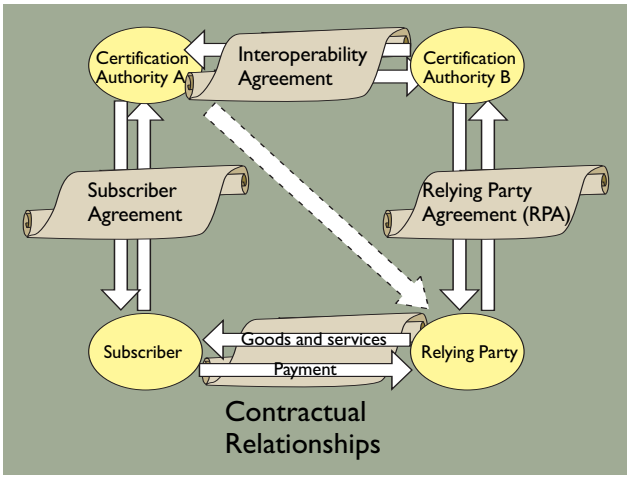
Information Asymmetry in the Certification Services Market

Akerlof [2] studied markets with informational gaps between buyers and sellers, and developed the "Lemons principle" as a generalized theoretical framework for understanding the dynamics of markets with information asymmetry. He argues that the cause of information asymmetry lies in imperfect information distribution between sellers and buyers. In this situation, the sellers have more information than the buyers about the true quality of goods. As a result, buyers assess the quality of the goods from the market as a whole and are led to assume that all goods in the market have the same average quality. The economic consequence would be that sellers have an incentive to market lower-quality goods for the same average price. This leads to better-quality goods not being traded in the market because their true value may not be obtained. Consequently, both the average quality of goods and the size of the market tend to fall.

We argue that the early headlong growth of trust services has led to quality uncertainty in this market. In a typical electronic transaction, trading parties might use digital certificates from different CAs as

WE ARGUE THAT THE EARLY HEADLONG GROWTH OF TRUST SERVICES HAS LED TO QUALITY UNCERTAINTY IN THIS MARKET.

their means of mutual reciprocal identification and authentication. In the marketplace, there exist many different certificate policy domains [9], each with its own certificate policy and practices for ascertaining identity. As a consequence of these variances in policy and practice, relying parties cannot be completely certain whether certificates issued by an unknown CA can be trusted and hence whether to rely on them. On the basis of this observation, we contend that the spread of CAs throughout the world, with their different procedures, technologies, and legal frameworks has contributed to the existence in the market of certificates of variable quality. Uncertainties in the quality of the digital certificates have an impact on the perception of trustworthiness of both the credential and the issuer. With no common agreed method for rating the quality of digital certificates, trust in extra-domain certificates can only be slowly and expensively constructed through a small number of given models, such as cross-certification, bridge CAs, and cross-recognition, each of which has its own shortcomings.



Contractual relationships in certification services.

We assert that consumer unfamiliarity with the use of digital certificates 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 the associated risks are. This creates an incentive for opportunistic behavior by some CAs to underinvest in technology and operational procedures for the creation and management of digital certificates, which in turn compromises the quality of certificates.

Following the same logic of argument as the "Lemons principle," we maintain that, in respect to certificates, there is asymmetry of information between the CA and the relying party. As a consequence, relying parties are unable to distinguish the quality of extra-domain digital certificates and hence must 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 may result in no incentive for the production of digital certificates of good quality in this market. After several iterations, in an extreme scenario, this might lead to only low-quality certificates existing in the market: the poor-quality certificates driving out the good. We recommend empirical studies to ascertain the accuracy of this assertation.

The Role of Quality Standards in the Certification Services Market

The problem of information asymmetry in markets can be circumvented or mitigated by different signaling mechanisms. Akerlof [2] identifies three countermeasures for quality uncertainty: licensing, brand names, and warranty. Backhouse et al. elaborate on how these signaling mechanisms can be applied in the PKI market [3]. In this article, we concentrate on the role of standards in addressing the problem of information asymmetry and of increasing the trust between trading entities in the context of electronic transactions.

Economists have researched the management and the consequences of standards strategy in market penetration and economic performance [10]. Concepts such as network externalities, lock-in management, and switching cost can be applied in analyzing the economics of standards. Standards that are widely implemented and adopted in the marketplace are known as de facto standards. One well-known de facto standard in the PKI market is RSA Laboratories' set of Public Key Cryptography Standards (PKCS) specifications. In contrast to de facto standards, de jure and consensus standards are those established with a purpose of interoperability, harmonization, and quality control. Standards of this kind are normally associated with official standards bodies such as International Organization for Standardization (ISO), and the Internet Engineering Task Force (IETF). One example of de jure standards in the PKI area is ISO/ITU-T X.509. Here, rather than viewing standards as a market strategy, our objective is to examine the role of de jure and consensus standards as a means of increasing the amount of information available to the relying parties for assessing certification quality, thus allowing quality control over the CA operation. With this control in place, the trust service market might prove a more viable and sustainable solution for facilitating trust in the context of e-commerce.

	Technology-specific approach	Technology-neutral approach	Two-tier approach
Key characteristics	adoption of asymmetric cryptography as the approved means of creating a digital signature; imposition of certain operational and financial requirements on certificate authorities, prescription of the duties of key holders; definition of the circumstances under which reliance on an electronic signature is justified	aims to facilitate the use of authentication technologies in general, with a motive of removing any existing legal obstacles to the recognition and enforceability of electronic signatures and records; limited to defining the circumstances under which an electronic signature will fulfill the existing legal requirements for tangible signatures.	acknowledge and promote the advantages of PKI in authentication, while not completely denying other types of authentication technology
Legal Guarantee	rigorous mandatory licensing or accreditation schemes to ensure CA in compliance with regulations	case law, the court is responsible for determining the legal admissibility and evidential weight of a given authentication technology	voluntary CA licensing schemes
Examples of operating countries	Argentina, Germany, India, Italy, and Malaysia	Australia, Canada, Finland, New Zealand, U.S.	Hong Kong and Singapore

Table 2. Regulatory approaches.

In the field of PKI, among the de jure and consensus standards, we consider that there are three types of quality-assurance standards: technical, best practice, and regulatory oriented. Technical standards ensure smooth operation and transmission between computers while best practice and regulatory standards offer trading parties confidence in the interoperability and enforceability of trust relationships across policy domains. In a dynamic marketplace, relevant technical standards and best practices are mostly developed or proposed by practitioners, and some later are adopted by standardization bodies, as indicated in Table 1. On the regulatory side, there are no universally agreed standards, but instead three legislative approaches are recognized for lending legal authority to the electronic authentication mechanism [1, 12], as presented in Table 2. These approaches include: prescriptive, neutral, and two-tier. Table 2 highlights the differences and provides examples of countries where these approaches are pursued. A prescriptive approach typifies, through compulsory licensing schemes, governmental intervention for assuring relying parties that all CAs meet the minimum quality requirements. A neutral approach leaves the decision to case law, the court being responsible for determining the legal admissibility and evidential weight of a given authentication technology. With the two-tier approach, relying parties are able to make a judgment of CA quality with the aid of an optional CA licensing scheme. Currently, even in countries that utilize a technology-neutral approach, such as the U.S. and Australia, WebTrust and the Gatekeeper accreditation schemes are employed to alleviate the problem of information asymmetry between CA and relying parties.

The Economics of Quality Standards

The preceding section examined technical and legislative approaches for regulating the operation of the certification services market. From our perspective, to ensure a minimum quality of certification service, we argue that the focus should be more on the economic dimension than the technical. Compared with regulatory standards, technical standards are easier to agree upon and to implement. By contrast, the regulatory dimension is more complicated, given its nature and the number of direct users. Thus, we consider that in order to increase the effectiveness of regulatory standards as signaling devices for CA quality, a number of issues must be addressed.

The first issue is the process of information dissemination and education. In markets other than certification services, the use of minimum quality standards has a long history so that consumers in general are more knowledgeable about their existence and function. For instance, in the professional services market of lawyers and accountants, many citizens have knowledge about the types of licenses or examinations that lawyers or accountants are required to obtain. In the PKI market, by contrast,

TO ENSURE A MINIMUM QUALITY OF CERTIFICATION SERVICE, THE FOCUS SHOULD BE MORE ON THE ECONOMIC DIMENSION THAN THE TECHNICAL.

the development and use of standards is a very recent phenomenon and as a result relying parties may be unaware of the existence of the minimum quality standards even in their own jurisdiction, let alone in others. Only when there is a critical mass of users that understands such standards or accreditation schemes can effective use be made of such devices to signal the CA quality distribution in the market.

The second concern is the question of interoperability. We argue that in e-commerce, the deployment of and reliance on digital certificates easily spans multiple policy domains, thus the use of signaling devices needs to do likewise. In the previous section, we asserted that a country may adopt one of three different legislative approaches. Furthermore, there are variances in the evaluation criteria that apply to existing CA licensing schemes, aggravating the problem of standards interoperability at the international level. Indeed, we now have the economics of imperfect information making itself felt in the minimum quality standards market. Certificate users may be aware of minimum quality standards in their own jurisdiction, but might not have information regarding the quality of a licensing scheme that the extra-domain CA may have in reality satisfied. Applying the model for information asymmetry, relying parties might assume that all minimum quality standards are the same. This would result in the ineffectiveness of standards as signaling devices for CA quality.

The third concern is that de jure standards can indicate quality if they introduce a degree of homogeneity in products and services in the certification services market, and hence the assurance of a minimal quality standard. However, we believe that the number and variety of different de jure standards may not lead to the desired effect. In a dynamic marketplace, reaching agreement on de jure standards may be impossible, and ultimately contribute to confusion rather than providing assurance.

Conclusion

This article has examined both the problems of, and possible countermeasures for, quality uncertainty in the current certificate services market. We have argued from an economic perspective that the asymmetry of information between the certificate authorities and the relying parties has contributed to the slow growth in this market. We have demonstrated this argument by using the "Lemons principle" and applying the principle to analyze the certificate services market. Furthermore, the effectiveness of quality standards when addressing quality uncertainty has been evaluated: these standards are only effective if they are perceived and understood by all parties involved in the market.

Despite these problems and the low adoption rates, it is too early to dismiss PKIs, as they have become embedded into identity management systems and e-government services. This article has presented an economic perspective on the market for such services and on the development of standards to support them. C

References

1. Aalberts, B. and Van Der Hof, S. Digital signature blindness analysis of legislative approaches to electronic authentication. *The EDI Law Review 7*, 1 (2000), 1–55.
2. Akerlof, G. The market for 'lemons': Quality uncertainty and the market mechanism. *Quarterly Journal of Economics 89* (1970), 488–500.
3. Backhouse, J., Hsu, C., Baptista, J., and Tseng, J. C. The key to trust? Signaling quality in the PKI market. In *Proceedings of the 11th European Conference on Information Systems* (Naples, Italy, 2003).
4. Camp, L.J. and Lewis, S., Eds. *Economics of Information Security*. Kluwer Academic Publishers, Boston, 2004.
5. Clarke, R. Privacy requirements of public key infrastructure. *Internet Law Bulletin 3*, 1 (2000), 2–6.
6. Ellison, C. and Schneier, B. Ten risks of PKI: What you are not being told about public key infrastructure. *Computer Security Journal*, XVI (2000).
7. Ford, W. and Baum, M.S. *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*. Prentice Hall, Upper Saddle River, NJ, 1997.
8. Gordon, L., Loeb, M., and Sohail, T. A framework for using insurance for cyber risk management. *Commun. ACM 46*, 3 (Mar. 2003), 81–85.
9. Lloyd, S. et al. CA-CA interoperability. PKI Forum TWG, 2001.
10. Shapiro, C. and Varian, H. *Information Rules: A Strategic Guide to the Network Economy*. Harvard Business School Press, Boston, 2002.
11. Spyrelli, C. Electronic signatures: A transatlantic bridge? An EU and U.S. legal approach towards electronic authentication. *Journal of Information, Law, and Technology 2* (2002); elj.warwick.ac.uk/jilt/.
12. Wilson, S. A comparison of authentication technologies in e-business. *The Asia Business Law Review* (July 2001).

James Backhouse (james.backhouse@lse.ac.uk) is a senior lecturer in Information Systems and the director of the Information Systems Integrity Group at the London School of Economics and Political Science.
Carol Hsu (cwy_hsu@yahoo.com.tw) is a manager for International Business Affairs at Taiwan Securities Central Depository and a part-time visiting assistant professor in the Management Information Systems department at National Chengchi University in Taiwan.
Jimmy C. Tseng (jtseng@rsm.nl) is an assistant professor of Information Security in the Decision and Information Sciences department at RSM Erasmus University in Rotterdam, The Netherlands.
John Baptista (j.m.baptista@lse.ac.uk) is a teaching assistant in the Information Systems department at the London School of Economics and Political Science.

The U.K. Economic and Social Research Council provided grant support in the Fiducia project L142251004, Modeling the Risks of Interoperable Public Key Infrastructures, where a part of this research was conducted.