PANEL IV: CERTIFICATION, AUTHENTICATION, AND ELECTRONIC SIGNATURES

Moderator: Ira Rubinstein[A]
Panelists: Stewart Baker,[B] Otavio Carlos Cunha Da Silva,[C]
Ronaldo Lemos Da Silva,[D] Jordi Masias,[E]
Jorge Muñiz Ziches,[F] Benjamin Wright[G]

Rapporteur: Susan-Jacqueline Butler[H]

Ira Rubinstein

Electronic commerce (e-commerce) involves an analysis of how strangers are doing business online with the use of the Public Key Infrastructure (PKI), a public key-based technology that includes digital signatures and supporting services such as certification authorities (CA) and their certificates. PKI assumes three parties: the subscriber, the certification authority, and a relying party. Initially, the subscriber requests a certificate from the certification authority. To obtain a certificate, the subscriber has to enter into a contract with the certification authority that governs the issuance of a certificate. Finally, the relying party depends on the certificate to verify the identity of a subscriber in connection with a message signed by the subscriber. Regarding the role of these parties in an online transaction, it is important to keep in mind that there are basically two different kinds of transaction models: the open PKI model and the closed PKI model.

The open PKI model is characterized by the non-existence of a relationship between the certification authority, the subscriber, and the relying party. The certification authority vouches for the personal identity of a "stranger"–the subscriber. The certification authority links with its certificate a public key and an individual subscriber. Accordingly, the certification authority creates rules for confirming the unique identity of its subscribers. Any subscriber may obtain a certificate by following the certification authority's rules. A single certificate is issued to the subscriber, who uses it for diverse purposes with a wide range of parties. In the open PKI model the certificates are verifying personal identity to some level of trust, and thus allow strangers to enter into agreements.

In the closed PKI model there is a pre-existing relationship between the certification authority and the subscriber, for example a corporation and its employees, trading partners, or a bank and its customers. Here the certification authority vouches for some specific characteristic or relationship of a subscriber. The issued certificate is linking a public key and some attribute or privilege, for example employment status, access rights, or membership. The certification authority leverages existing databases to identify employees, customers, and members or relies on a preexisting relationship with a subscriber, which already

defines rights and responsibilities. Only certain individuals with the characteristic or relationship in question may request and obtain a certificate. The subscribers are likely to hold a number of certificates and use them in specific, narrow contexts. In the closed PKI model, certificates are enabling technology, but they do not necessarily establish identity because not all of the varied uses involve personal identity.

In the open PKI as a business model, third parties rely on a certificate because they trust the issuing certification authority and because they have recourse against it. The costs of a certificate to a user reflect the level of security and other available protections. The certificate authority being marginally cost sensitive would raise its prices to its customers if costs become higher due to regulatory requirements. On the other hand, the closed PKI as a business model has little if any third-party reliance. The certificates are free or very cheap to users. The certification authority is price sensitive and would stop issuing certificates if costs become too high due to regulatory requirements the authority would be unable to pass along additional costs to customers.

In creating a legal framework for e-commerce, governments should consider the following: the types and uses of certificates including non-identity certificates, the various transaction models and their underlying assumptions about identity, the various business models and the economics of issuing and using certificates within each model, the risk allocation and its effect on liability, and the authentication methods that are not dependent on PKI technology.

Stewart Baker

Authentication through electronic signature is an important e-commerce topic because . . . "on the Internet, no one knows you're a dog." To do serious business on the Internet, identification of the other party is important. In addition, sometimes doing business requires getting the customer's "signature."

One kind of electronic signature is PKI technology, which is asymmetric cryptography. This digital signature technology works on a "key" system, with a public key that could be published anywhere and a private key that must be kept secret. Described in a simplified way, the sender of a computer message encrypts her message with the private (secret) key, known only to the sender. The recipient of the message uses the more widely known public key of the sender to decrypt and to read the message. Only the public key can decrypt messages encrypted with the private key and vice versa. Thus, this system also can be used for the purpose of authentication. If someone encrypts a message with her secret key and it can be decrypted with her public key, the message must have come from the secret key holder. This system also provides confidentiality because someone can send a message even to a stranger and encrypt this message with the stranger's public key. Only the stranger, holding the private key, can decrypt the message with her private key. Typical implementation is the relying party, the signing

party who is the holder of the private key, and the certifying authority who publishes the public key.

Can this electronic authentication system be defeated? There are two main problems. First, a digital signature can be forged by stealing the private key or corrupting the certification authority. Second, the signer could deny that her signature is valid. She might use the factual excuse that she was sloppy with her private key or that somebody else used it, or she might use the legal argument that it is not a legal signature, but is just a bag of bits.

However, there are suggestions to these problems. First, legal obligations should be created to minimize technology's flaws. Accordingly, the practices and liabilities of the certification authorities must be defined and clear. The signing party must have clear responsibility to prevent or communicate any compromise of the private key. Secondly, the electronic signature has to be recognized as equivalent to a handwritten signature.

Electronic signature laws have progressed through two generations. There are the prescriptive legislative solutions, a first-generation type, such as those chosen by the states Utah and Washington, and the countries Germany and Italy. This could be considered as a good solution if there is only one government. Prescriptive rules, such as Germany's security standards, could also invalidate contracts.

Second-generation laws are emerging "two-tier" solutions with basic recognition for all electronic signatures and more benefits for higher security and regulatory approaches that can be found in Singapore's regulations or in the European Union directive. Presently in the United States, there is a two-tier solution as well as just the bottom tier solution with a basic recognition. The top tier will present more of a trade problem, such as can now be found in Germany and Italy, which are discriminating against non-European Union states and the European Union directive, which requires international agreements. The United Nations Commission on International Trade Law (UNCITRAL) Rules are a possible solution.

Otavio Carlos Cunha Da Silva

Although most people think that e-commerce means online shopping, this is only a small part of e-commerce. E-commerce also includes bank-to-bank and business-to-business transactions, such as connections that make purchases easier for big corporations. E-commerce is implemented on the Internet, a network designed for openness and not for security, whereas e-commerce demands a high level of security.

The National Technology Readiness Survey, illustrates that e-commerce creates considerable concern to the public. Consumers are worried about privacy and security of online transactions. A high percentage of consumers do not feel confident doing business with a place that can only be reached online. Consumers

are also worried about giving out a credit card number online. A majority would prefer to have their online transactions confirmed in writing. Accordingly, success in cyberspace will be determined by how well these issues will be addressed.

Thus, the key issue for e-commerce in the future is online security. So far, it has been the foremost hindrance to online shopping in Brazil. Businesses are anxious about unauthorized purchases and theft through impersonation. Consumers are worried about the security of transmitting private information that could be intercepted or misused.

E-commerce will not be fully embraced by users until there is trust that services and networks are secure and reliable; transactions will be safe and private; there will be ways to prove the origin, receipt, and integrity of information received; and identity of the parties involved is known. Furthermore, there have to be appropriate redress mechanisms available if something goes wrong.

The main security concerns for e-commerce, besides providing non-repudiation, are those of availability, confidentiality, and integrity of information systems as well as of the data that is stored and transmitted. Accordingly, cryptography is important as a security measure; it provides for the integrity of e-commerce transactions and helps to gain trust of online consumers. Confidence of users in electronic transactions can be built by the development and use of authentication and certification technologies and mechanisms. Digital authentication technology is contributing to the growth of e-commerce by providing a method of establishing trust between participants of online transactions. Digital certificates improve security concerns in non-commercial transactions by authorizing access to key information sources without passwords, by providing non-repudiation of messages sent over the Internet, and by verifying the integrity of information.

An issue to be considered is the conflicting national solutions for electronic authentication and certification, which could have an impact on the development of global e-commerce. Also important are cross border cryptography, digital signature, and certification. Security solutions should be simple to be implemented and cost effective. They should have the capacity to seamlessly integrate with the existing business environment.

Ronaldo Lemos Da Silva

Despite the immense growth of e-commerce, Brazil has not enacted any kind of legislation regulating e-commerce. The Brazilian legal system already embodies principles and provisions suitable for e-commerce. Thus, the questions to be raised are: Should there be specific regulations for e-commerce? And if so, how to regulate e-commerce?

Considering the current law in Brazil, Mr. Lemos identified two shortcomings: the lack of specific regulations of evidence for electronic documents and electronic signature, which leads to a high level of uncertainty; and the impossibility of notarizing an electronic document that is a requirement for certain transactions. Further, a set of draft bills has been presented to the Brazilian Congress in order to eliminate these deficiencies. Recently, the Brazilian Bar Association presented one draft bill to the Brazilian Congress. While drafting this bill, international experiences had been considered, such as the UNCITRAL Model Law, the European Union Directive, and the Utah Digital Signatures Act.

The draft bill regulates three issues: e-commerce, electronic signatures, and electronic documents. It grants certain presumptions relating to electronic documents that have been electronically signed and where the signature has been certified by a certification authority. These presumptions are important because they are shifting the burden of proof. Therefore, these presumptions reduce the uncertainty regarding evidence relating to electronic contracts.

However, there are also problems arising out of this draft bill. First, the draft is only regulating one specific kind of electronic signature–the PKI model. It is not technologically neutral, thus other types of electronic signatures are not receiving the same benefits of presumptions. In addition, it has to be considered that the PKI model is not infallible. Applying the draft bill, the party using the private key would be entitled to the legal presumptions. If this key is used by an unauthorized person the authorized key holder has the burden of proof that her key has been misused.

Who can qualify as a certification authority? According to the draft bill only Brazilian public notaries should be entitled to serve this function and only their certificates would enjoy the legal presumptions. But notary services in Brazil are not rendered in a marketing fashion and are subject to certain appointments by the government. Thus, the structure cannot be characterized as being an efficiency-aimed institution. As an illustration, big cities like Sao Paolo, with approximately ten million inhabitants, have only thirty notaries. He pointed out that e-commerce requires a very efficient and timely service structure. Certification services not only register public keys but also have to revoke them immediately in certain situations.

As a consequence, the proposed regulations are not efficient to foster e-commerce development in Brazil. His concern is that regulations could create new obstacles in the future and hinder the development of e-commerce in Brazil.

Jordi Masias

Jordi Masias introduced the Chamber of Commerce in Barcelona along with its purposes and functions. Observation of the market and of new technologies is crucial to keep companies competitive. The Internet is improving

competition, but it is poorly organized and there are security concerns. Consequently, there are initiatives to overcome these deficiencies.

He also introduced the Digital Certification Service of the Chambers of Commerce, CamerFirma, one out of four certification entities in Spain. Its purpose is to define and offer a high-quality digital certificate, especially designed for the needs of companies. It is issuing digital certificates for businesses, particularly business-to-business transactions. It has international recognition based on the guarantee related to the issuance by a Chamber of Commerce. CamerFirma is based on the ChamberSign trust Network with initially ten national associations from European countries (Germany, Austria, Belgium, Spain, France, the Netherlands, Italy, Luxembourg, the United Kingdom, and Sweden) and Eurochambers participating. The system will be expanded through the Worldwide Network of Chambers of Commerce. Further information is available at http://www.cambrabcn.es.

Jorge Muñiz Ziches

E-commerce raises security and legal issues. In his opinion the digital signature is of magnificent importance and might be the key to solving both the security and legal concerns. In Peru, draft bills are pending on e-commerce and digital signature that closely follow the UNCITRAL model.

One of the most important issues is to determine when a contract is perfected, even though it presently seems that the business world is not considering this problem. E-commerce needs regulations and international cooperation. In addition, it requires the education of judges and other court members in the subject of e-commerce and the creation of an international court. In the meantime, e-commerce disputes should be solved through arbitration.

Benjamin Wright

Everybody should be aware that there is already a variety of technology for authentication purposes available and it is important to keep in mind that while some enterprises succeed, others do not. Experience is short and therefore policymakers should be humble.

A. Ira Rubinstein graduated from Yale Law School in 1985. He currently heads Microsoft's Electronic Commerce Group in Law and Corporate Affairs with responsibility for worldwide electronic commerce policy including encryption, digital signatures, privacy, and critical infrastructure issues. Mr. Rubinstein is an active participant in international discussions of electronic authentication and encryption policy through both the International Chamber of Commerce (ICC) and the Business and Industry Advisory Committee (BIAC) to OECD. Over the past few years, he has attended meetings of the UNCITRAL Working Group on Electronic Commerce, Vienna (1999); the OECD Ministerial Conference on A Borderless World–Realizing the Potential for Global

Electronic Commerce, Ottawa (1998); and the OECD Ad Hoc Group of Experts on Cryptography Policy, Paris (1996-1997), either as a member of the ICC or BIAC delegations. Mr. Rubinstein currently serves on the U.S. Department of Commerce, President's Export Council, Subcommittee on Encryption (PECSENC). He is also the author of annual survey of export controls on encryption software for the Practicing Law Institute and is a frequent speaker at legal and public policy seminars.

B. Stewart A. Baker graduated from UCLA School of Law in 1976. Mr. Baker practices law at Steptoe & Johnson LLP in Washington, D.C. From mid-1992 to mid-1994, he was General Counsel of the National Security Agency, where he was actively and publicly involved in issues such as export controls and key-escrow encryption. His work in the private sector involves a variety of high-tech, mass media, privacy, and telecommunications issues, with an emphasis on international and appellate matters. Mr. Baker is a member of the President's Export Council Subcommittee on Encryption, a member of the Free Trade Area of the Americas Experts Committee on Electronic Commerce, and a member of the UNCITRAL Group of Experts on Digital Signatures.

C. Otavio Carlos Cunha Da Silva graduated with a degree in Electronic Engineering, Business Administration and Economics, and received a postgraduate degree in Policy and Management of the Research and Development Process and in International Commerce. He is presently working in the area of Information Security for the Brazilian Government–Presidency of the Republic since 1983, with emphasis in the area of cryptographic applications.

D. Ronaldo Lemos da Silva, Jr. graduated from the University of Sao Paulo Law School, Special Training Program (PET-CAPES) sponsored by the Ministry of Education in 1999. He is Teaching Fellow of Jurisprudence and General Theory of Law at the University of Sao Paulo Law School, and is an attorney with Suchodolski Advogados Associados practicing in the areas of telecommunications, e-commerce, tax, international law, and contracts. He authored a chapter on Brazil in the book *The Law of International On-line Business–A Global Perspective*, Sweet & Maxwell, London, 1998. He has made contributions to Brazilian and foreign publications, such as the INTER-AMERICAN TRADE REPORT published by NLCIFT. He is an Honorary Member of the Center for International Legal Studies, Salzburg, Austria, and a member of the Brazilian Bar Association.

E. Since July 1993, Jordi Masias has been responsible for the Information Technology Services Department of the Barcelona Chamber of Commerce. Under his leadership, the Chamber recently initiated a program to provide digital certification services to businesses in Barcelona and will soon launch an aggressive electronic commerce awareness campaign for small and medium-sized businesses that will run through the year 2000. The electronic commerce project is a key priority for the Barcelona Chamber of Commerce because eighty-five percent of businesses in the region of Catalunya are small and medium-sized businesses. Mr. Masias is currently Chairman of the Eurochambers Technical Group for Business Digital Certificates and also an active member of the Eurochambers Working Group on Telecommunications. He has also participated in the DEMARCHE (1998) and MAGICA (1996-1997) European projects, both supported by the European Commission.

F. Jorge Edgar Muñiz Ziches graduated from Pontificia Universidad Catolica del Peru, with a Bachelor of Letters and Human Sciences (1971). He received a Bachelor of Laws from the same university with the presentation of a thesis entitled "Interpretation of Contracts" that was graded as Outstanding (*summa cum laude*). In 1976 he obtained the professional degree of Attorney-at-Law before a jury, also with the grade of Outstanding

(*summa cum laude*). Since 1991 he has served as President of the National Commission for Foreign Investment and Technology (CONITE). Since November 1, 1992, he has served as President of the National Institute for the Defense of Competition and the Protection of Intellectual Property (INDECOPI). Mr. Muñiz Ziches is an elected member of the Peruvian Congress for the period 1995-2000, was appointed Chairman of the Congress Justice Commission for the period 1995-1996, is a member of the Congress Permanent Commission, and more recently, Chairman of the Commissions charged with the reform of the Commercial and Civil Codes.

G. Benjamin Wright is the author of *The Law of Electronic Commerce*, a comprehensive book on the legality of electronic contracts, published by Aspen Law & Business. He is Editor Emeritus of the *Journal of Electronic Commerce*, where he served part time as editor 1992-98. A graduate of Georgetown University Law Center, Mr. Wright is an independent attorney practicing electronic commercial law in Dallas, Texas. Since 1988 he has delivered over four hundred speeches on e-commerce and been quoted in publications around the globe, from the WALL STREET JOURNAL to the SYDNEY MORNING HERALD. Mr. Wright's expertise extends beyond strictly legal matters. He advises clients about the design and function of electronic commerce technologies so as to achieve optimum legal results. He is named as a co-inventor on a pending e-commerce patent application sponsored by one of his clients. For the past five years he has advised an electronic signature company, PenOp, Inc., on product marketing, advocacy and development.

H. Susan Butler received her First State Examination (law degree) in 1989 from the Christian-Albrechts-Universitaet in Kiel, Germany. As a law student she worked as a research assistant for Professor Samson at Christian-Albrechts-Universitaet and continued to work for him as a teaching assistant after graduation until 1992. In 1992 she started the legal internship (Referendarszeit) that is a prerequisite for the Second State Examination. After passing the Second State Examination in the summer of 1994, she worked as a lawyer in Kiel, becoming a partner of the law firm in January 1997. She earned the degree of a specialist in administrative law. Mrs. Butler is a candidate for LL.M., University of Arizona College of Law, 2000.