Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 13-Dec-1999
Dist. : 15-Dec-1999

English text only

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(99)14/FINAL
Unclassified

Working Party on Information Security and Privacy

JOINT OECD-PRIVATE SECTOR WORKSHOP ON ELECTRONIC AUTHENTICATION

Stanford and Menlo Park, California
2-4 June 1999

English text only

85545

ACKNOWLEDGEMENT

The OECD and the private sector alliance co-ordinated by the Business and Industry Advisory Committee to the OECD (BIAC) would like to thank the contributors, sponsors and hosts that have made this workshop possible: The Governments of Canada, Germany and the United States (the latter which has provided funding for interpretation services), The Stanford Program in Law, Science & Technology of Stanford Law School and SRI International (which together hosted the meeting at their facilities), The Electronic Frontier Foundation (EFF) (which hosted a reception on 2 June at Stanford Law School), RSA Data Security and IBM (which together hosted a reception and dinner on 3 June at Thomas Fogarty Winery), Morrison & Foerster LLP, Oracle Corporation, VISA International, Charles Schwab, PricewaterhouseCoopers and Steptoe & Johnson LLP.

TABLE OF CONTENTS

OVERVIEW

Information security issues are a vital concern for developing electronic commerce, and a number of initiatives are underway in both the public and private sectors to ensure that businesses and consumers can engage in secure and reliable electronic communications and transactions in the global networked society. The OECD's recent work in this area has focused on electronic authentication issues. In recent years OECD Member countries have undertaken to develop and implement policies and laws related to authentication and electronic signatures. Disparities in policy may create obstacles to the evolution of national and global information and communications networks and hinder the development of electronic commerce. Both governments and the private sector in Member countries have recognised the need for international collaboration to develop an efficient and secure information infrastructure. The OECD is playing a role in this regard by providing a forum for exchange of views and developing consensus about specific policy and regulatory issues related to information and communications networks and technologies, including electronic authentication.

The OECD Working Party on Information Security and Privacy is comprised of government and private sector representatives from OECD Member countries. It has conducted work related to authentication for a number of years. Both the 1992 *OECD Guidelines for the Security of Information Systems* and the 1997 *OECD Guidelines on Cryptography Policy* note the importance of data integrity and security in information and communications networks and systems. The OECD Inventory of Approaches to Authentication and Certification in a Global Networked Society surveys activities in OECD Member countries related to authentication and certification on global networks, including laws, policies and initiatives in the public and private sectors, and at both the national and international level. A "Declaration on Authentication for Electronic Commerce" adopted by Ministers at the Ottawa Ministerial Conference in October 1998 recognizes the importance of authentication for electronic commerce and outlines a number of actions to promote the development and use of authentication technologies and mechanisms, including continuing work at the international level, together with business, industry and user representatives. Ministers declared their determination not to discriminate against the authentication approaches taken by other countries and to amend, where appropriate, the technology or media specific requirements in current laws or policies that might impede electronic commerce.

This Joint OECD-Private Sector Workshop on Electronic Authentication was held on 2-4 June 1999 in Stanford and Menlo Park, California. The one-half day pre-meeting technology primer looked at basic examples of the use of authentication in electronic transactions, including a description of the various technologies and models for electronic authentication and how they work, and a discussion of the role of authentication in electronic transactions. The two day workshop looked at business and government models for implementing electronic authentication; the approaches of different industry sectors; and the requirements for the international operation of global authentication systems. The workshop was aimed at continuing the open dialogue among OECD Member countries on global electronic authentication mechanisms as technologies, business models and policies continue to evolve. The discussion at the workshop was framed around a number of public and private sector case studies that were used as a mechanism for exchanging information and highlighting developments in the field in order to identify and clarify public policy issues related to electronic authentication.

This Joint OECD-Private Sector Workshop was organised under the auspices of the Information, Computer and Communications Policy Committee's Working Party on Information Security and Privacy, and in co-operation with private sector representatives. However it was not a formal meeting of any OECD subsidiary body. The members of the APEC Telecommunications Working Group were also invited to participate in the workshop. The OECD Secretariat worked with a steering committee comprised of representatives from Member governments, the private sector, international organisation partners, and consumer advocacy and user organisations to finalise the agenda, select appropriate speakers and determine the topics for analytical papers. Private sector participation was organised through the Business and Industry Advisory Committee (BIAC) to the OECD, which brought together a coalition with wide private sector representation to co-operate in the workshop planning.

More than 200 participants attended the workshop including national delegations of Member countries; members of the APEC Telecommunications Working Group; private sector representatives, including the business and industry coalition co-ordinated by BIAC; consumer and user representatives and NGOs, including public interest groups from the domains of consumer protection and civil rights; international organisation representatives; and the OECD Secretariat and experts designated by the Secretariat.

The workshop was not designed to yield any conclusion or recommendation out of the discussion. However, through the workshop, it was made clear that the authentication technologies were still rapidly evolving, although some were used widely. Mentions were made of policy and technical challenges in specific applications. However, it was repeatedly stressed that no single technology was universally applicable to the existing diverse business and government models considered.

AGENDA

Pre-Meeting Technology Primer
2 June 1999 (afternoon only)

Stanford Law School
559 Nathan Abbott Way, Crown Triangle, Room 290
Stanford, California

THE CONTINUUM OF APPROACHES TO AUTHENTICATION: A TECHNOLOGY PRIMER

The technology primer looked at basic examples of the use of authentication in electronic transactions, including a description of the various technologies and models for electronic authentication and how they work, and a discussion of the role of authentication in electronic transactions.

Stephen Kent, Chief Scientist of GTE Internetworking
Masanobu Higashida, Executive Manager, Security Project, NTT Information Sharing Platform Laboratories
Henry Beker, CEO, Zergo-Baltimore

Technology Discussion Panel

Moderator: Russell Housley, Spyrus Corporation
Speakers:

- Brian O'Higgins, Executive Vice President, Chief Technology Officer, Entrust Technologies (PKI)
- Warwick Ford, Verisign (PKI)
- Jim Bidzos, Security Dynamics
- Barbara Fox, Security Architect, Microsoft (Internet browsers)
- Gisela Meister, Giesecke & Devrient (smart cards)
- Kenneth Watson, Cisco (routers)

Question and Answer Session

3-4 June 1999
Stanford Research Institute, Menlo Park, California

- Norman Reaburn, Chairman of the OECD ICCP Committee's Working Party on Information Security and Privacy and Deputy Secretary, Attorney General's Department, Australia
- Ed Zeitler, Senior Vice President, Information Security Services, Charles Schwab

3 June 1999

OPENING SESSION

- Welcome by John Dryden, Head of the Information, Computer and Communications Policy Division, OECD
- **Keynote** by Professor Margaret Jane Radin, Co-Director of the Stanford Program in Law, Science & Technology, Stanford Law School
- **Introductory remarks** by Workshop Co-Chair Norman Reaburn, Chairman of the Working Party on Information Security and Privacy and Deputy Secretary, Attorney General's Department, Australia
- **Introductory remarks** by Workshop Co-Chair, Ed Zeitler, Senior Vice President, Information Security Services, Charles Schwab

SESSION I. UPDATE ON RECENT DEVELOPMENTS IN ELECTRONIC AUTHENTICATION

This session provided an update on recent developments in this field at the global and regional levels, with examples of specific private sector and government activities.
Moderator: Teresa Peters, OECD Secretariat
Speakers:

- Eiichi Yoshikawa, Chairman of the authentication group of the Global Business Dialogue on Electronic Commerce (trends in private sector initiatives in electronic authentication)
- Christopher Kuner, Morrison & Foerster (trends in national legislation)
- Richard Schlechter, DG XIII, European Commission (the EC Directive on electronic signatures)
- Steve Orlowski, Electronic Authentication Task Group, Asia Pacific Economic Cooperation (APEC) (work of the APEC electronic authentication task group)
- Jenny Clift, United Nations Commission on International Trade Law (UNCITRAL) (UNCITRAL's work on authentication)
- Dr. Walter Fumy, Chairman of ISO SC27 (securities technologies : trends in private sector standards initiatives)

Question and Answer Session

SESSION II: SECTOR CASE STUDY ON AUTHENTICATION IN FINANCIAL AND OTHER BUSINESS SERVICES

This session looked at authentication mechanisms and systems used in the electronic delivery of services, including banking, financial and other types of business services. Because of the nature of service industries where the lines between business-to-business and business-to-consumer communications and transactions are not always clear, this session looked at both

kinds of applications, including examples of the use of electronic authentication in online payments, online stock trading, and consumer banking.
Moderator: Brian W. Smith, Mayer, Brown & Platt

Speakers:

- Paul Wing, ScotiaBank
- Yoshikazu Kobayashi, INGECEP, Japan
- Roland Brandel, External Counsel for Indentrus
- Jari Nyholm, Merita Nordbanken Data
- Sigrun Erber-Faller, German Federal Notary Association
- William Kennair, Scrivener Notary; Chairman, CyberNotary Association, United Kingdom

Intervenor comments:

- Dominic Davison-Jenkins, J&H Marsh & McLennan (risk analysis and management)
- Richard Field, Attorney at Law (consumer issues)
- Martine Briat, Legal Department, Groupement des Cartes Bancaires
- William A. Barouski, United States Federal Reserve Bank
- Toshiyuki Miyoshi, Computer Communications Division, Ministry of Posts and Telecommunications, Japan

Question and Answer Session

Lunchtime Sessions
Presentations: (two separate presentations ran simultaneously in different rooms)

- Case study on Australian Government internal PKI experience: Adrian McCullach, Gadens Lawyers and Anne Caine, Deputy Australian Government Solicitor
- Digital signature technology for wireless networks based on the SIM card: Harri Vatanen, Sonera SmartTrust

Presentations: (two separate presentations ran simultaneously in different rooms)

- European Electronic Signature Initiative (EESSI): Hans Nilsson, ID2 Technologies
- Biometrics: Infinecon

SESSION III: ORGANISATIONS-TO-INDIVIDUAL TRANSACTIONS
This session looked at examples of authentication being used for electronic communications and transactions between commercial entities and individuals (e.g. in "business-to-consumer" electronic commerce), and between government agencies and individuals (e.g. in electronic delivery of government services), through the presentation of public and private sector case study examples followed by a discussion panel.
Moderator: Claude Boulle, Groupe Bull

Sector Case Study: Business-to-Consumer Transactions
Presentations:

- Andreas Mitrakas, Senior Legal Consultant, Globalsign
- Lennart Malmström, Sweden Post
- Ira Rudenstein, Microsoft

Sector Case Study: Electronic Delivery of Public Services by Government
Presentations:

- Ari Saapunki, Finnish Population Registry Centre
- Lauri Pesonen, SETEC
- Clare Wardle, UK Post Office Legal Services and Jeremy Hilton, JH Consulting

- Katarina DeBrisis, Ministry of Labour and Government Administration, Norway,
- Yeow Meng Chee, Assistant Director, International Office, National Computer Board, Singapore

Discussion Panel
Moderator introduction
Intervenor comments:

- Michael Baker, Executive Director, Asia Oceania Electronic Messaging Association (SME perspective)
- Caspar Bowden, Foundation for Information Policy Research

Question and Answer Session

4 June 1999

OPENING SECOND DAY
Chairman's welcome, administrative announcements

SESSION IV: ORGANISATION-TO-ORGANISATION TRANSACTIONS
This session looked at examples of authentication being used for electronic communications and transactions between commercial organisations and other commercial organisations (e.g. in "business-to-business" electronic commerce), and between government organisations and commercial organisations (e.g. in government procurement), through the presentation of public and private sector case study examples followed by a discussion panel. It will include a discussion of how electronic authentication is used in internal organisation operations.
Moderator: Peter Ferguson, Industry Canada
Sector Case Study: Electronic Authentication in Business-to-Business Communications and Transactions
Presentations:

- Bhaskar Kakulavarapu, Manager Advanced Technology, Lear Corporation (Automotive Network Exchange)
- Bill Tiga Tita, Chambre de Commerce et de l'Industrie de Paris (SMEs)
- Ken Fitzpatrick, Business Line Manager, PKI Security, IBM

Sector Case Study: Electronic Authentication in Government Transactions
Presentations:

- John Weigelt, Senior Technical Advisor PKI Task Force, Government of Canada
- Richard Guida, PKI Steering Committee, US Government
- Lionel Vodzislawsky, Ministry of Economy, Finance and Industry, France (project for electronic declarations for VAT and customs)

Discussion Panel
Moderator introduction
Intervenor comments:

- Peter Stokes, Deputy Chief Operations Officer, Tradelink (SME perspective)
- Jacques Pantin, CEO, Certplus
- Robbert Fisher, PriceWaterhouseCoopers

Question and Answer Session
LUNCH WITH SPEAKER
Speaker: Andre Reisen, Ministry of the Interior, Germany (technical specialist on German Digital Signature Law)

SESSION V: GLOBAL POLICY ISSUES
This session provided an opportunity for moderators from each of the previous panels to speak briefly about the issues of interest or concern that were brought out in case studies and presentations during the previous sessions. These remarks were followed by a panel discussion of global authentication in the context of the Ottawa Ministerial Declaration on Authentication for Electronic Commerce, looking at how the principles of the Declaration had been implemented in the case studies and the lessons to take away. The discussion was launched with comments from each of the workshop co-chairs, and it included time for questions and comments.
Session Moderator: Stewart Baker, Steptoe & Johnson

Discussion Panel: Reflection on Case Studies
Previous session moderator comments:

- Teresa Peters, recent developments
- Brian W. Smith, services case study
- Claude Boulle, organisation-to-individual case study
- Peter Ferguson, organisation-to-organisation case study

Discussion Focus: Global Authentication in the Context of the OECD Ottawa Ministerial Declaration
Presentations:

- Workshop Co-Chair Norman Reaburn, Chairman of the Working Party on Information Security and Privacy and Deputy Secretary, Attorney General's Office, Australia
- Ed Zeitler, Senior Vice President, Information Security Services, Charles Schwab

Intervenor comments:

- Andrew Pincus, Department of Commerce, United States [invited]
- Masanobu Kato, Internet Law and Policy Forum
- Hubertus Soquat, Ministry of Economics and Technology, Germany
- Dr. Supraya Singh, Centre for International Research on Communication and Information Technologies (CIRCIT), Australia (consumer issues) [invited]
- Fuminori Inagaki, Ministry of International Trade and Industry, Japan
- Laurent Jacques, Ministry of Justice, France
- Joseph Alhadeff, Oracle Corporation

Question and Answer Session

CLOSING REMARKS BY SECRETARIAT
John Dryden, Head of the Information, Computer and Communications Policy Division, OECD

RAPPORTEUR'S REPORT

Session I. Opening Session

Speakers

- Ms. Margaret Jane Radin, Co-Director, Program in Law, Science, and Technology, Stanford Law School.
- Mr. Norman Reaburn, Workshop Co-chair; Chairman, OECD ICCP Committee's Working Party on Information Security and Privacy; Deputy Secretary, Attorney General's Department, Australia.
- Mr. Ed Zeitler, Workshop Co-chair and Senior Vice President, Information Security Services, Charles Schwab.

Margaret Jane Radin, Keynote

Following welcoming remarks by John Dryden, Head of the OECD's ICCP Division, Ms. Radin gave the keynote address. Ms. Radin began by observing that we face a new era which presents a variety of challenges, and that as we develop a framework for electronic commerce, it is important to consider what is best left to free markets and what is best left to government.

Ms. Radin went on to discuss the evolution of views regarding the government's role with respect to the Internet. She first noted the early "romanticisation" of the Internet and the "no regulation" sentiment that often accompanied that view, then discussed the shift away from that view. She observed that free markets cannot exist in a state of anarchy because governments establish certain prerequisites for free markets (*e.g.*,reasonably clear property rights). Ms. Radin therefore suggested that the real questions are, "When does a governmental organisation need to structure interaction?" and "How can intranational, national, and international government bodies work together with private organisations?"

Ms. Radin identified authentication as the linchpin of electronic commerce, explaining that electronic authentication systems nurture the security of transactions. She called attention to the broad range of authentication technologies at different stages of development and the diverse nature of electronic transactions (*e.g.*,business-to-business; business-to-consumer; government-to-constituents). She also noted the plethora of legislative initiatives involving digital signatures and other forms of electronic authentication (*e.g.*,each state of the United States has enacted, or has pending, digital signature legislation, and there are initiatives pending at the federal level).

On the basis of these observations, Ms. Radin concluded that the issue of standardisation is an urgent one. She explained that for electronic commerce to flourish, a way to arrive at standardisation is needed. She suggested that the challenge to be faced is how best to do so. In particular, the tension is that we want

competition, not monopoly, yet we seek to honour countries' different traditional approaches. Ms. Radin ended by noting that the OECD and its private-sector partners are addressing this question.

Norman Reaburn, Co-chair

Mr. Reaburn began by stating that his is a "government perspective". He noted that the Ottawa Declaration recognised the importance of e-commerce. The declaration's purpose is to *i)* establish a dialogue between business and government, *ii)* identify where governments need to act, and *iii)* facilitate the exchange of information on approaches to authentication. Its five key principles are *i)* to avoid discrimination; *ii)* to facilitate the use of technologies and mechanisms for electronic commerce; *iii)* to amend, where appropriate, technology or media-specific requirements in current laws or policies that may impede the use of electronic authentication mechanisms; *iv)* to apply electronic authentication technologies to enhance the delivery of government services to the public; and *v)* to continue work at international level with business, industry, and user representatives concerning authentication technologies and mechanisms to facilitate global electronic commerce. The OECD's Working Party on Information Security and Privacy (WPISP) has already developed a declaration on privacy in networked environments and the goal of the workshop was to try to draw out more of these issues.

Mr. Reaburn pointed out that the meaning of authentication has shifted since the Ottawa discussions. At that time, the term "authentication" was used to mean public key cryptography. Today, the term is no longer restricted to this technology; more is involved.

As Mr. Reaburn explained, the joint OECD-private sector workshop was to take a bottom-up approach, relying on case studies of the use of electronic commerce. While government is always tempted to impose solutions, the bottom-up approach helps to ensure that any government approach addresses articulated needs and does not involve constant changes of position.

In addressing appropriate roles for government, Mr. Reaburn felt that government should use authentication technology for its own services. In addition, it should encourage the use of electronic commerce ("put some yeast in the mix").

Ed Zeitler, Co-chair

Mr. Zeitler remarked that Schwab was an early technology adopter, as the brokerage business is well suited to electronic commerce. The firm's clients are technologically sophisticated and have taken to electronic commerce *en masse*. He explained that, as a result, Schwab has been heavily involved in electronic commerce issues. As the brokerage business is highly regulated, Schwab has pushed the limits on government regulation.

Mr. Zeitler identified authentication as a key issue for electronic commerce, but noted that the views of only a few years ago do not fit today's world. To be successful today, different communities have to play various roles. As Mr. Steve Kent stated in his presentation on 2 June, different certification authorities (CAs) should have a multitude of spans of authority.

After noting that government has a role to play, Mr. Zeitler discussed that of the private sector. The private sector specialises in change, both in technology and in the market. It relies on trial and error; companies try something, and if they are unsuccessful, they try something else. Today's successful businesses "cannibalise" their own customers. In the past, companies were reluctant to introduce new products when they had a successful product used by many customers. Today, they do not hesitate to do so, so that other companies do not get the market.

In practical terms, Mr. Zeitler stated that, although ScotiaBank representatives may disagree, most electronic authentication systems do not work. Consumers may not be ready for electronic authentication, and, in particular, they may not be ready for a card that can replace them in legal transaction. Consumers currently have credit cards, but the associated risk is not very great. A card containing their legal identity, one that would legally bind a person, is perhaps more than they are willing to contemplate.

Noting that the principles being developed in various high-level organisations, such as the OECD and the Internet Law and Policy Forum (ILPF), are converging, Mr. Zeitler suggested that further work needs to be based on experience. With regard to the role of OECD, he concluded that it is critical for the OECD to continue to press for non-discrimination in laws, services, and products. The OECD can be of real value to the business community and the world at large by taking "the walk down the middle" between the private sector and the government sector. Finally, Mr. Zeitler emphasised the need for the private sector and governments to have the time necessary to work out their issues.

Recent developments in electronic authentication

Moderator

- Teresa Peters, OECD

Speakers

- Eiichi Yoshikawa, Senior Vice-president of NEC Corporation; Chair of the Authentication and Security Issues Group of the Global Business Dialogue on Electronic Commerce (GBDe)
- Christopher Kuner, Attorney-at-Law, Morrison & Foerster LLP
- Richard Schlechter, DG XIII, European Commission
- Steve Orlowski, Electronic Authentication Task Group, Asia-Pacific Economic Cooperation (APEC)
- Jenny Clift, United National Commission on International Trade Law (UNCITRAL)
- Dr. Walter Fumy, Chairman of ISO SC27

Teresa Peters, OECD

Ms. Peters spoke first about the OECD's *Inventory of Approaches to Authentication and Certification in a Global Networked Society*. The inventory surveys OECD Member country activities related to authentication and certification on global networks. The survey includes information about law, policy and various initiatives in the public and private sectors at both national and international levels. For example, it covers approaches such as certification that go beyond identity and non-user-linked authentication (computer-to-computer authentication). The inventory serves as a tool for information exchange among Member countries, and Ms. Peters invited the private sector to contribute to it.

Ms. Peters explained that, as part of the survey, OECD Member countries were asked to answer questions such as: *i)* What types of laws does your country have, and how are these laws being applied?; *ii)* Are your country's laws technology- and media-neutral (as required by UNCITRAL)?; *iii)* Do you allow contractual arrangements? (in general, private contractual arrangements are allowed); *iv)* How are CA issues being handled? Are CAs being accredited, and if so, on what is accreditation being based?; *v)* What problems

arise with global, cross-border transactions? Ms. Peters noted that Member countries identified questions focusing on global transactions as being most difficult.

Ms. Peters concluded by stating that, in light of the results of the workshop, WPISP would consider its future work in the area of electronic authentication at its meeting on 5 June 1999.

Eiichi Yoshikawa: Trends in private sector initiatives in electronic authentication

Mr. Eiichi Yoshikawa began by describing the GBDe. It is an industry-led initiative that aims to foster a predictable environment for the future development of electronic commerce. The Authentication and Security Issue Group of GDBe is one of nine issues groups (the others are Consumer Confidence, Content/Commercial Communications, Information Infrastructure, Intellectual Property rights (IPR), Jurisdiction, Liability, Protection of Personal Data, and Tax/Tariffs). The Authentication and Security Issue Group will be making proposals at the GBDe plenary meeting in Paris in September 1999.

The Authentication and Security Issue Group is composed of private-sector participants whose twin goals are: *i)* to ensure that trust in electronic transactions is as great or greater than trust in traditional transactions; while *ii)* familiarising people with the use of new technology. The group's initial discussions culminated in a draft, which was discussed via e-mail. The first draft was posted on the Web on 10 February 1999. Companies and organisations from all over world made comments. There were 8 000 "hits" a month on the Web site, 50 people were on the mailing list and 40 concrete comments were posted to the mailing list. Discussion closed on 10 May 1999, and the group is editing the final draft.

In elaborating on the group's discussions, Mr. Yoshikawa highlighted four areas: *i)* development of authentication systems and services; *ii)* establishment of electronic signature laws; *iii)* development of use of cryptography; and *iv)* promotion of government procurement.

In terms of development of authentication systems and services, there should be a variety of systems and services. In addition, authentication levels should be rated to fit the value of the transaction. Industry should take the lead in setting market-based standards, criteria, guidelines and rules. Since electronic commerce is essentially a global matter, governments should not take a discriminatory approach to other countries' authentication. Finally, governments should make an effort to promote market entry based on market demand.

With regard to the establishment of electronic signature laws, Mr. Yoshikawa made several points. First, electronic signatures should have the same effect as a written signature or a personal seal (used in several Asian countries), but government should avoid excessive intervention so as not to obstruct private-sector activities. In addition, laws should not hinder the development of technology.

With respect to the development of the use of cryptography, Mr. Yoshikawa stated that this is the private sector's responsibility. Strong cryptography is essential to the security of an information society and will serve individuals, governments and businesses. Government should not restrict distribution, export or use of strong encryption and should not force service providers to undertake management or key escrow.

Finally, Mr. Yoshikawa drew attention to the idea that government should take a leadership role in the use of electronic commerce and identified government procurement as a core driving force.

Christopher Kuner: Trends in national legislation

Mr. Kuner first described three different types of regulation of electronic signatures: national legislation, national administrative regulation, and state regulation. The trend toward national electronic authentication legislation was triggered by the passage of the Utah Digital Signature Act (a US state law). Since the Utah law was passed in 1996, a number of countries have passed, or are considering, some form of legislation or regulation. Indeed, legislation has been enacted in almost every region of the world (*i.e.* Asia, Europe, North America, South America) and there is much pending legislation as well. In addition to national legislation, there are some national administrative regulations governing electronic authentication. For example, in the United States, the Federal Reserve and the Food and Drug Administration (FDA) have regulations regarding the use of electronic authentication methods. Finally, there is state digital signature legislation (now called electronic signature or electronic authentication legislation). State legislation is important in federal systems such as the United States.

Mr. Kuner next identified three approaches to electronic authentication legislation: the prescriptive approach, the two-tier approach, and the minimalist approach. Prescriptive legislation, which tends to be the earliest, is limited to the use of digital signatures within a public key infrastructure. Two-tier legislation bestows basic legal benefits on all electronic authentication mechanisms, but offers broader benefits for "approved" technologies. This approach is taken by Illinois (United States) and Singapore and can be seen in some UNCITRAL work. Finally, some legislation takes the minimalist approach. It does not have detailed standards but focuses on granting basic legal recognition and removing barriers to electronic authentication. This approach is evidenced in the Australian approach and in many recent US state laws.

Mr. Kuner next discussed legislative activity in Europe: Germany and Italy were the first in Europe to act, and legislation is imminent in other EU member states. Electronic authentication in Europe will likely have a three-tiered structure in the future, with top-level, mid-level, and low-level security.

In the United States, Mr. Kuner continued, federal laws enacted in 1998 will promote the use of electronic authentication in government paperwork. In addition, several federal agencies (*e.g.*,the FDA) have passed regulations enabling the acceptance of electronic signatures for governmental transactions. All states will soon have electronic authentication legislation. Currently, there is no uniformity of legislation among the states. Prescriptive, Utah-style schemes are out of favour, and there is a trend towards technology-neutral legislation. Cross-border recognition remains a problem. There are several bills pending in Congress, and more federal legislation will likely be enacted.

In concluding, Mr. Kuner noted that, worldwide, legislation tends to be parochial, focusing on the country in which it is written.

Richard Schlechter: The EC Directive on electronic signatures

Mr. Schlechter first said that the motivation for the Directive was that Germany, Italy and other member states were actively developing electronic signature laws, and the EC was concerned about the prospect of divergent national laws. The six main principles embodied in the Directive involve: *i)* technology neutrality; *ii)* limited scope; iii) market access; *iv)* legal recognition; *v)* liability; and *vi)* cross-border provisions.

Limited scope. The Directive does not apply to closed systems or user groups, such as a corporate intranet or a banking network, where it can be assumed that a contractual, or at least a trust relationship, already exists. There is only one exception: electronic signatures used within closed systems will also be allowed to benefit from legal recognition.

Market access. No prior authorisation is required to enter the market, but voluntary accreditation schemes are permitted. A certification service provider (CSP) can enter the market and issue services without accreditation. At the same time, countries can establish voluntary accreditation schemes and have different administrative systems. Thus, they can have systems based on a self-regulatory scheme with governmental supervision.

Legal recognition. The Directive requires member states to ensure that advanced electronic signatures (linked to requirements for certificates, CSP and signature creation devices) are recognised as satisfying the legal requirement for a signature in the same way as handwritten signatures and that they are admissible as evidence in legal proceedings. In addition, it is not permissible to discriminate against electronic signatures solely on that grounds that they are electronic.

Liability. Service providers are liable for all information included in a certificate, but they can limit liability by limiting the value of transactions or the scope for which the certificate can be used. The Directive embraces the principle of negligence, which provides that the service provider must act negligently to be liable. However, the burden of proof is on the service provider, who must prove lack of negligence.

Cross-border provisions. The Directive provides for non-discrimination (including for certificates coming from third countries) and legal recognition (Article 7). An electronic signature based on a third-country certificate could be legally recognised in the EU if, for example, a service provider outside the EU found a service provider within the EU willing to serve as a guarantee for his certificates.

Mr. Schlechter indicated that the expected time frame for adoption and implementation of the Directive was to have final adoption by the end of 1999. Implementation at national level will be required by the beginning of 2001.

Steve Orlowski: Work of the APEC Electronic Authentication Task Group

Mr. Orlowski outlined a series of business models for authentication, identified various authentication techniques, and described a set of certification models.

In March 1999, the APEC Electronic Authentication Task Group prepared an issues paper and is preparing technical annexes for that paper. The cross-certification sub-group is examining the possibility of cross-certification between APEC member countries. As part of its work, the Task Group observed how businesses were using authentication as they went online and identified three business models for authentication, which varied depending on the relationship between the transacting parties.

These business models can be described as open, closed and open but bounded. Each has different implications for liability and security. In the open model, there are no prior arrangements between transacting parties, which are separate entities. The parties often rely on a third party, and there may be a legal agreement between one of the parties and the third party. The classic example of the open model is Internet business: two parties may enter into a transaction without any prior contact or formal arrangement. Indeed, this is the traditional Internet trading model, and three years ago it was thought that authentication would operate in this way.

In the closed model, authenticators are exchanged between parties with a pre-arranged contractual or organisational relationship which extends to the issue and use of authenticators. There is a prior agreement between the transacting parties, and they may be part of a single legal entity. Examples of the closed model of authentication include the value-added networks (VANs) used for electronic data interchange (EDI) and

Internet shopping or banking using a pre-agreed authentication technique. A system is also closed where there is direct agreement with a central node or a relationship between each of the parties to a transaction.

Finally, in the open-but-bounded model, an authenticator is recognised, but there is not necessarily a direct relationship or agreement between the parties. In this model, many parties could rely on an authenticator, but limits would be placed on the number of those parties, and trust would be gained through advance agreements among known parties. Examples of this model include situations in which one transacting party has a direct agreement with a party, another transacting party has a direct agreement with a different party, and the transacting parties have a general agreement that they will recognise each other's authenticators. A simpler example is that of a user clicking the "I accept" button, thereby creating a general agreement (for that transaction) between the sender and the receiver.

Mr. Orlowski next mentioned various authentication techniques, including asymmetric cryptography, shared secret cryptography, biometrics, and other, less formal techniques (*e.g.*,domain names e-mail, universal resource locator – URL). He also noted the availability of hybrid authentication techniques. For example, a hybrid system might combine biometric authentication with digital signatures based on asymmetric cryptography.

He then drew attention to the existence of a range of certification models: the formal (hierarchical) model, the informal (web of trust) model, cross-certification, cross-recognition, and no certification. The cross-recognition model provides enough information for a party to agree to accept certificates from other parties without the formal cross-certification process which requires the mapping of certificate policy (CP) and the certification practice statement (CPS). Thus, cross-recognition provides a lower level of certification than cross-certification.

The Task Group's next steps will be to co-operate with international bodies such as the OECD, complete the technical annexes mentioned above, and attend the electronic authentication workshop in Lima in September 1999. Mr. Orlowski stated that, from APEC's perspective, whatever is done in terms of policy and legislation must focus on the transaction as a whole.

Jenny Clift: UNCITRAL's work on authentication

Ms. Clift stated that when preparing its Model Law on Electronic Commerce, UNCITRAL had recognised authentication as one of the most important issues for promoting electronic commerce. Given the predominance of public key cryptography, UNCITRAL has focused its work on digital signatures, but it recognises that other authentication techniques should not be discouraged. In terms of public key cryptography, the UNCITRAL Working Group saw that model rules might need to deal with various levels of security and to recognise the various legal effects and levels of liability corresponding to the services provided in the context of digital signatures. The Working Group was also aware that there was value in market-driven standards for certification authorities and that a minimum set of standards might be valuable, particularly in the context of cross-border certification.

Ms. Clift noted that the UNCITRAL Working Group had difficulty reaching a common understanding of the new legal issues arising from the use of electronic signatures and had yet to reach consensus about the legislative policy on which rules should be based.

She then mentioned views that have been expressed about the Working Group's work and discussed the group's future focus. One concern was that the current approach did not sufficiently reflect business needs for flexibility in the use of electronic signatures and other authentication techniques. Another was that most of the pressing issues relating to the use of electronic signatures were solved by the basic legal recognition of electronic signatures in the Model Law on Electronic Commerce, so that nothing more was needed at

this point. This was especially the case in the field of commercial law, where party autonomy should be emphasised. The prevailing view, however, was that the work of the Working Group should continue on the basis of its existing mandate. Indeed, countries are looking to UNCITRAL for guidance in preparing their legislation. The Working Group is to focus not on a specific model, but on three functions: those of key holder, certification authority and relying party. A number of delegations thought that the imposition of a time frame might galvanise the Working Group, but as this was not generally agreed, the group will continue its work on an open basis. A working paper would be posted on the UNCITRAL Web site at the end of June 1999.

Dr. Walter Fumy: Security technologies: trends in private-sector standards initiatives

Dr. Fumy first alluded to a recent comment about the multiplicity of standards before turning to various authentication options. These include, for messages, the block cipher and the hash and, for entities, passwords, techniques based on block cipher, message authentication code (MAC), and digital signature, as well as zero-knowledge techniques.

In describing various trends in authentication, Dr. Fumy recalled that there has been a shift from block cipher-based message authentication (*e.g.*,based on data encryption standard – DES) to message authentication based on hash functions/MAC. There also has been a shift from secret to public key authentication (although, as Dr. Fumy noted, third-generation mobile phones rely on authentication schemes based on a secret key). In addition, within public key cryptography, there is a trend away from reliance on the RSA (Rivest, Shamir, Adelman) algorithm towards greater reliance on elliptic curve cryptography, which offers more security per bit than either RSA or DSA (digital signal algorithm), so that it is particularly well-suited to low power or low bandwidth applications. Two standards currently cover elliptic curve DSA (ECDSA), and additional standards are in the pipeline on elliptic curve cryptography. Finally, there is a trend away from reliance on passwords and personal identification numbers (PINs) and towards biometric authentication.

At this point, there was a discussion of the scope of the electronic signature Directive. Mr. Schlechter had earlier stated that the data protection provisions of the European Commission's Directive did not apply to closed user groups. To clarify, he said that a CA that signs up its clients is not a "closed user group". When asked how one differentiates between a bank operating as a CA and a CA operating as a CA, Mr. Schlechter explained that the Directive applies as soon as certificates are issued to the public. If a bank issues certificates within an existing relationship, the bank is not offering anything to the public, and therefore does not come under the Directive. In contrast, a bank falls under the Directive if it issues certificates not only to clients that the bank already has, but to the public.

Mr. Schlechter also noted, with respect to non-discrimination, that, in principle, there are no obstacles to certificates coming from third countries to Europe under the electronic signature Directive. The Directive's only requirements are for service providers within Europe. The problem is how to ensure that a service provider within a third country will abide by these requirements.

Finland noted that there is a data protection provision in the Directive on electronic signatures and asked if it is essential, for digital signatures, to say something about data protection. Mr. Schlechter responded that it is not essential for electronic signatures to discuss data protection. He explained that the data protection provision is a response to the problem of the use of pseudonyms. The Directive includes the data protection article (*i.e.* specific provisions for data protection) so that people can use pseudonyms in a certificate.

Session II: Authentication in Financial and Other Business Services

Moderator

- Brian Smith, Mayer, Brown & Platt

Speakers

- Paul Wing, Vice-president, Systems Security and Control, ScotiaBank
- Yoshikazu Kobayashi, INGECEP, Japan
- Roland Brandel, External Counsel for Identrus
- Jari Nyholm, Merita Nordbanken Data
- Sigrun Erber-Farber, German Federal Notary Association
- William Kennair, Scrivener Notary; Chairman, CyberNotary Association, United Kingdom

Intervenors

- Dominic Davidson-Jenkins, J&H Marsh & McLennan, Risk analysis and management
- Richard Field, Attorney-at-Law, Consumer issues
- Martine Briat, Legal Department, *Groupement cartes bancaires*
- William Barouski, US Federal Reserve Bank
- Toshiyuki Miyoshi, Computer Communications Division, Ministry of Post and Telecommunications, Japan

Before introducing the speakers and intervenors, Mr. Smith drew attention to a gap between business activities and governmental action. Businesses tend to face similar legal, technical and social concerns. He suggested that electronic commerce requires a policy environment that fosters international competition, technical competition, and non-discrimination among solutions and law.

Paul Wing, ScotiaBank

Mr. Wing discussed the authentication aspect of ScotiaBank's online banking system. He began by recalling that authentication is a fundamental of banking (*e.g.*,need reliably to verify who obtains money and information and from whom money and information are received; need to know if instruments of value are authentic). Therefore, strong, effective authentication is a requirement for safe online operation. To ensure secure electronic commerce over the Internet, the Bank of Nova Scotia (BNS) was an early adopter of public key infrastructure (PKI) technology. The Bank can control the PKI, so it can manage risk effectively.

Mr. Wing then focused on the authentication aspect of the Scotia online system. The system has two components: the Scotiacard and public-key-based digital signatures. The Scotiacard identifies ScotiaBank customers and serves as an automatic teller machine (ATM) card and as a card for Internet-based services. Public-key-based digital signatures are a vital component of secure electronic commerce because they provide strong mutual authentication.

Mr. Wing then described four design aspects of Web-based banking and discount brokerage services: enrolment/registration; customer-controlled passwords/passphrases; anonymous certificates; and single sign-on. First, to enrol, a customer calls an 800 number and, after satisfactorily answering "skill-testing" questions (*e.g.*,questions about one's credit record), the customer is given a shared secret to use to create a certificate. The customer-controlled password is used to encrypt secure information at the customer's desktop and is not sent over the Internet or over an internal network. Passphrases serve the same purpose, but are easier for customers to remember and less costly to administer; they are phrases, of unlimited length, from which the vowels are removed. Developed by ScotiaBank in conjunction with entrust, an anonymous certificate does not specifically name or identify the owner or subject of the certificate, thereby limiting the risk of certificate misuse. Note that in all ways (except one) anonymous certificates are in X.509 format. The final design aspect is single sign-on.

Yoshikazu Kobayashi: INGECEP/CyberNet

Mr. Kobayashi spoke about INGECEP (Integrated Next Generation Electronic Commerce Environment Project). It is a pilot project for next-generation electronic commerce under the auspices of APEC. Its objective is to contribute to the development of electronic commerce in APEC regions by identifying obstacles and sharing the outcome of its work among APEC members. INGECEP focuses on the cross-border environment and cross-border electronic commerce, and one of its main goals is to build user trust and confidence.

INGECEP is concerned with a series of issues, including security, quality of goods, privacy of information and consumer protection and convenience. It has adopted two solutions to protect consumers in the cross-border environment. First, the Secure Electronic Transaction (SET) protocol is used to protect consumers from eavesdropping and forgery. Second, electronic authentication is used to solve the repudiation problem.

Mr. Kobayashi then discussed the procedure used for electronic payment (debit). First, the clearinghouse receives a payment instruction from a consumer. It then sends a request for payment to the consumer's bank account. After confirming receipt of goods by the consumer, INGECEP notifies the bank, which then transfers the payment. There is a prearranged contract between the bank, the clearinghouse and consumers. INGECEP has developed a contract agreement between the consumer and the clearinghouse (debit agreement) and has developed another for use between the shop and the consumer.

The procedure for secure issuance of certificates is as follows. First, the consumer sends an application over the Internet. INGECEP then sends the consumer the necessary forms, including a debit agreement form between the consumer and the bank. The consumer signs the agreement with a seal. INGECEP receives the direct debit agreement and sends it to the bank to verify the authenticity of the seal (*i.e.* it is the one on record with the bank). If the seal is correct, INGECEP sends the software and a user ID and password. The consumer then installs the software, generates private and public keys, and requests a certificate. If all the information is correct, a certificate is issued on the Internet.

In conclusion, Mr. Kobayashi stated that building consumer trust is important, that the solutions adopted by the INGECEP pilot system are effective in building consumers' trust and confidence, and that the trust placed in the CA and clearinghouse depend on social recognition and the achievements of the operators. He added that it is difficult for some Internet users to obtain a digital certificate, but as electronic authentication based on public key cryptography is one of the most effective methods now available for ensuring telecommunications security, its use is likely to expand in the future. Finally, he noted the need for quick solutions to the legal issues that plague electronic authentication, such as the legal effects of electronic signatures and the issue of mutual international recognition of CAs.

Roland Brandel: Identrus

Mr. Brandel began by describing Identrus. It is a Delaware LLC owned by large banks including the Bank of America, Bankers Trust, Barclays Bank, Chase Manhattan Bank, Citibank, Deutsche Bank, HypoVereinsbank. Its goal is to create a global, interoperable, digital certificate system by establishing a highly secure system for identifying parties over electronic networks, including the Internet. The Identrus project was initiated about a year and a half ago to try to handle certain issues, including cross-border certification (the need for a certificate issuer in one country to be trusted by people who need to rely on certificates in another) and risk allocation. Part of the cross-border certification problem involves dealing with a certificate issuer in a remote jurisdiction if the certificate is false, a problem which Identrus has addressed. Identrus deals with the risk allocation problem by permitting a relying party to shift identity risk to the certificate issuer by purchasing a warranty.

Identrus is a business-to-business system and was designed to deal with large commercial transactions. It is technologically neutral. Although it currently uses a PKI-based system, it might look to other solutions in the future. Identrus participants may choose among a variety of technology vendors. Identrus is also application-neutral. Although the participants are banks at present, Identrus is not intended exclusively, or even primarily, for financial applications and can be used across a wide range of applications. Finally, it was designed as a closed system, in which interlocking contracts are associated with every entity involved. The interlocking contractual relationship is similar to the international bank card model (*e.g.*,Mastercard), in which two banks do not have a direct contractual relationship but follow common operating procedures and risk allocation principles.

After recalling that there can be no product or service unless the provider is willing to assume some liability, Mr. Brandel described how Identrus deals with risk. In the Identrus system, the issuance and validation of a certificate generally do not mean that the certificate issuer incurs liability. However, the issuer may assume liability by associating a warranty with the certificate. If the certificate recipient wants the certificate issuer to shoulder financial liability, the recipient simply requests a warranty. The certificate issuer will then associate a price with that warranty, and the parties will either strike a bargain (*i.e.* there will be a warranty) or the issuer will not assume any liability. In addition to allocating risk using a warranty, Identrus isolates and controls risk. Identrus is different from bank card systems in that it is constructed to isolate risk to individual participants and builds specific protections for those who rely on warranties.

Finally, noting that Identrus was designed to minimise transaction costs and maximise efficiency, Mr. Brandel explained that Identrus relies not on the judicial system, but on arbitration of claims regarding certificates. This approach to dispute resolution provides the necessary “quick reaction time”.

Jari Nyholm: Merita NordBanken Data, Finland

Mr. Nyholm discussed NordBanken’s PKI-based security solution for private customers using the Internet for banking services, which was launched in 1997. The project is used for private customers and has not yet been expanded to corporate customers. To use the system, one must be a customer of NordBanken and have Windows NT, a CD-ROM, a mouse, and an agreement with an Internet service provider (ISP).

To address the need for strong authentication, NordBanken relies on a smart card with photo identification, which serves both as a visual identification card and as an electronic identification (EID) card over the Internet. The EID contains two separate and unique private RSA keys, is PIN-protected and contains the corresponding public keys with X.509 certificates.

The procedure for obtaining the smart card is as follows. First, the customer comes to a bank office, in person, to fill out an application. He or she must provide the clerk with a photo identification, which the clerk checks. The clerk then signs a form and sends it to the card manufacturer with an ISDN (integrated services digital network) connection to the Nordbanken system. The card manufacturer generates four keys, of which two public keys go to Nordbanken, which certifies them and returns them to the manufacturer. The latter then puts a PIN on the card, sends the customer the PIN and sends the customer back to the bank with his/her electronic ID card and a CD-ROM. The public telephone company gives the customer a card reader, and the customer installs the CD-ROM and card reader. The CD-ROM provides the software needed to make the system work. NordBanken uses the CD-ROM to deliver the latest browser, NordBanken's certificate and the software needed to interact with the system. For security, both the server and the client are authenticated using SSL (secure sockets layer) v. 3.0 with 128-bit encryption.

Sigrun Erber-Faller: German Federal Notary Association

Ms. Erber-Faller explained that notaries are legal professionals as well as public officers whose profession is regulated by law. She said that the use of electronic means is expected to have a variety of benefits for notarial practice, as an analysis of notarial business cases and notarial communication (*e.g.*,electronic land registers) demonstrates.

Ms. Erber-Faller described a pilot project which focuses on electronic communication and the use of digital signatures. In the first and simplest scenario, online access to the database of the German Notarial Institute is provided through a closed network, so that there are no legal implications. In addition, there are no form requirements and no external partners to complicate the situation. A second, more complicated scenario provides for communication between notaries and notarial professional bodies. Finally, the Notary Association plans to expand the project, ultimately providing advanced inquiry procedures with regard to the public land register.

Ms. Erber-Faller identified several cases in which electronic communication might be used in notarial practice, including the electronic filing of applications to state registers, a central data file for wills, electronic inter-office communication and expansion of electronic communication to public authorities, courts and clients in order to cover as many aspects of the transaction as possible.

In terms of the technical design of Notary Association's notarial communication infrastructure, the secure infrastructure will be based on a virtual private network (VPN) with protected Internet access. In addition, the association will create a notarial certification authority and use hardware and software in accordance with the Digital Signature Law. The "bad news" is that the Digital Signature Law precludes the association from purchasing the hardware and software on their own because it is too expensive. The "good news" is that the security level is high enough to use it as it is for the association's purposes.

In conclusion, Ms. Erber-Faller noted that terms of reference are currently being established and a call for tender is expected soon at European level.

William Kennair: Open Signature Certification Architecture (OSCAR) Project

Mr. Kennair undertook a practical review of the Open Signature Certification Architecture (OSCAR) Project. OSCAR is a collaboration between the computer industry and European notaries. Belgian, Spanish, French and UK notaries are involved. The perspective of the UK notaries is somewhat different from that of the others because the United Kingdom has a common law system and all UK notarial work is therefore international.

Mr. Kennair discussed the functional and the practical assessment of the OSCAR project. The functional assessment involved questionnaires answered by four notariates. Three notary associations (*i.e.* all but that of the United Kingdom) felt that communicating with the right persons was the real concern. The UK notary association, not surprisingly, was more interested in being able to certify documents which would be used in another jurisdiction. With respect to the practical assessment of the use of OSCAR software to sign a document, Mr. Kennair first described how the OSCAR software is used. First, one clicks on OSCAR and inserts a card (with 1024-bit RSA). OSCAR can then be used in two ways. In one, the notary acts as a CA and issues a public key certificate. Company A can then use the OSCAR software to sign a document, get a trusted time stamp and e-mail the document to Company B. The X.509 certificate is available from the "Properties" menu. Alternatively, A can create a document in the presence of a notary. Then, the notary puts a document around the original document and sends the whole package to B. In this approach, A, the consumer, does not need a personal key set. In the future, French notaries will be using OSCAR for certain purposes.

Dominic Davison-Jenkins, Intervenor

As a risk consultant and insurance broker at J&H Marsh and McLennan, a company whose client base is comprised mainly of Fortune 500 companies, Mr. Davison-Jenkins spoke about operational risk. He advises these companies about the risk of heavy involvement in electronic commerce. As his comments pertained to operational, not business, risk, his focus was on first- and third-party risk.

He began by discussing risk assessment, stressing the need to recognise and be sensitive to its importance. Without a proper understanding of risk, one cannot mitigate, allocate and finance risks. Further, it is important to recognise that risk identification and analysis has a great bearing on policy and law. As the consequences of a flaw are great, it is important to obtain information from lawyers and insurance companies that attempt to deal with risk.

In Mr. Davison-Jenkins' view, the world is seeing a revolution, a shift towards the knowledge-based economy. As a result, electronic risk profiles are very complicated, because people are doing old things in new ways and new things for which there are no precedents. In the latter case, there are few statistics, so it is hard to determine what can go wrong and what the cost would be. Legal uncertainties also contribute. A good method is for those closest to the risk to deal with it. People should ask, "What can go wrong?" and "Who should pay for liability and how bounded should it be?" That is, if something goes wrong (in practice, it will not often happen), who pays?

Finally, Mr. Davison-Jenkins focused on the importance of insurance. Noting that insurance pooling made possible maritime trade, the last great expansion of trade, he suggested that, today, insurance will make the financing of risks possible and some insurance products will deal with consumer confidence issues.

Richard Field, Intervenor

Mr. Field, representing the consumer perspective, addressed four issues: privacy issues, access, risk allocation and the necessity of non-repudiation.

In terms of the privacy aspects of authentication systems, Mr. Field referred briefly to two systems already described. He noted that ScotiaBank must possess personal information to complete the "skill-testing" aspect of enrolment and questioned where those data go. He added that Identrus may have a lot of personal data but it is not clear how the data are managed.

In his discussion of access issues, Mr. Field mentioned the need to consider access by the disabled, blind and elderly. It may be necessary to develop simplified solutions for them and this may be required by law in the United States and other countries.

Next, in Mr. Field's view, the goal of risk allocation from a consumer perspective is to attain systemic reduction of risk without undue government oversight. Indeed, the issue of how to allocate risks fairly so as to lead over time to systemic risk reduction without undue government oversight is an important consumer issue. The problem of risk allocation in authentication stems from the fact that no authentication system is perfect. For example, the PKI approach has glaring weaknesses (*e.g.*,issuance and loss of certificates), and biometric systems have weaknesses as well. However, in combination, some of these technologies will minimise systemic risk. The challenge is to encourage those able to improve the system to do so. While self-regulation is excellent because it allows for experimentation, the incentive of self-regulation is to shift risk to the consumer or to those who did not develop the system and are unable to improve it or minimise systemic risk.

Finally, he addressed the need for non-repudiation. Mr. Field noted that Mr. Kobayashi had said that non-repudiation was necessary. His view was that non-repudiation may not be the piece of security that the consumer wants.

Martine Briat, Intervenor

Ms. Briat raised two issues: neutrality (non-discrimination) and data privacy.

On the first, Ms. Briat explained that, in France, in case of a dispute, the judge has to evaluate which certificate is best. The issue has come up; there is a case pending in France in which a cardholder alleges that he had a valid instruction to pay. Not only does the cardholder want to be sure that any payment instruction he/she gives to a bank has been executed, the Court needs to be sure that the instruction given by the cardholder was valid. In France, in order to determine the validity of the payment instruction, the judge must evaluate the validity of the certificate. Although the judge relies on expert testimony and the proceedings are lengthy, in the end, the judge must decide which certificate is the best.

French cardholders, Ms. Briat remarked, are reluctant to see data concerning them disclosed to a third party. She acknowledged that data on Internet trade are not very good but also that there are currently few Internet payments in France. This seems to be because many consumer cardholders will not make card transactions. She noted that she does not advise consumers to give card numbers over the Internet. In her opinion, the solution is secure transactions on the Internet and smart cards are a good means to that end. She noted that more standardisation (*e.g.*,smart card reader) is needed and congratulated the European Commission for standardisation of the reader because that is the first step towards fully secure electronic payment on the Internet.

William Barouski, Intervenor

Mr. Barouski stated that, from the perspective of a payment system or mechanism, the important characteristics of an electronic system include low cost, high security, ease of use, immediate finality, privacy, low risk, widespread risk, interoperability among systems and a universal payment standard. However, this list contains inherent conflicts, such as the tension between low cost and high security. He explained that while technological advances help address these conflicts, advances in regulation and payment laws are still needed.

Finally, selection of service will be based on the service (What do I get?), the cost (What do I pay?), and the risk (What can I lose?). After making this calculation, certain consumers just will not participate in electronic commerce.

Toshiyuki Miyoshi, Intervenor

Mr. Miyoshi began by noting that electronic delivery of services reduces transaction costs and maximises the use of the Internet in commercial activities. He then turned to the role of authentication in the electronic delivery of services. Authentication and encryption play crucial roles, notably for electronic commerce. However, development of authentication is still in the early stages.

Mr. Miyoshi then discussed the role of government. He said that the private sector basically should take the lead in this area, although government may facilitate its work by providing for collaboration, particularly at international level. Government facilitation might be especially important in Asian regions where government is expected to play a bigger role, as is the case in Japan as compared to North America and Europe.

Mr. Miyoshi concluded by describing some of the Japanese government's work on electronic commerce. First, the Ministry of Post and Telecommunications (MPT) proposed INTERCEPT as an APEC-registered project for providing cross-border electronic commerce in 1995. MPT also supports a field-trial e-cash service. It has a study group of experts on cryptography policy and authentication, with a report due for publication by the end of June 1999. Finally, MPT, the Ministry of Trade and Industry (MITI) and the Ministry of Justice (MOJ) are examining ways to promote electronic commerce and electronic authentication.

Session III: Organisation-to-Individual Transactions

Moderator

- Claude Boulle, Director of European Affairs for Groupe Bull; Co-chairman of the BIAC-ICCP Working Group on Authentication

In opening the session, Mr. Boulle noted that the previous session considered authentication of financial processes. Financial institutions were leading in the domain of business-to-business authentication. This session focuses on organisation-to-individual transactions. Mr. Boulle divided organisation-to-individual transactions into two component parts: business-to-consumer transactions and government-to-citizen transactions. Mr. Boulle noted that the presentations would deal first with business-to-consumer transactions and then with government-to-citizen transactions.

To start the business-to-consumer transactions discussion, Mr. Boulle noted that business-to-consumer transactions are a promising but emerging market. For example, GlobalSign currently receives less than 10% of its revenue from this area, which is, however, a promising one. Mr. Boulle then asked: "How do you see the business-to-consumer transaction market emerging and the business model for business-to-consumer transactions developing?"

1. BUSINESS-TO-CONSUMER TRANSACTIONS

Speakers

- Andreas Mitrakas, Senior Legal Consultant, GlobalSign
- Lennart Malmstrom, Manager, Business Development, Sweden Post
- Ira Rudenstein, Microsoft

Andreas Mitrakas, GlobalSign

Mr. Mitrakas of GlobalSign spoke about GlobalSign's business-to-consumer business, which involves, in particular, digital certificates for consumers. Before describing GlobalSign's services, he introduced the basic concepts on which these are based: digital identifiers (digital identities) and proofs (digital signatures). He explained that digital certificates bind together a public key and the identity of the certified entity, which may be a natural person, a legal person, a data object or a computer. Certificates are provided by CAs, which are trusted third-party entities that issue, publish, and revoke certifications. CAs may issue different classes of certificates depending on the level of trust.

GlobalSign is a CA, a European trusted third party. It also manages an international network of certification and registration authorities, all of which meet the same accreditation requirements. Thus, it manages a network whose aim is to meet the diversity typical of the European market. Further, GlobalSign's services are based on uniform rules in order to ensure interoperability. Indeed, GlobalSign's public certification services create a minimal common framework (based on EC Directives).

Mr. Mitrakas explained that the idea behind GlobalSign was to set up a clearing network and described its scope and volume. It covers seven EU and four Middle East countries and issued 120 000 certificates last year. Mr. Mitrakas confirmed Mr. Boulle's introductory remark that GlobalSign's business-to-consumer transactions account for just 10% of their revenue. He also noted that GlobalSign is involved in business-to-business projects related to consumers (*e.g.,*the Leganet network among Belgian lawyers that enables users to encrypt e-mail for confidentiality).

He then listed the requirements for obtaining a digital certificate. When an individual applies for a digital certificate, GlobalSign requests that he/she attest to certain facts: that the applicant rightfully holds the private key and that the information in the certificate is accurate. Certain of its procedures require the physical appearance of persons.

GlobalSign conforms to EC Directive 93/13 on the protection of consumers, which gives them the right to be informed and requires clear terms, use of the local language and full merchant responsibility. GlobalSign respects the rights of consumers as set by law.

In terms of liability and risk, GlobalSign is moving towards adopting certain warranties that will apply to all CAs in Europe. It provides assurance that a signature comes from a person with a signature creation device. It also plans to use liability caps and has an insurance policy related to certain contingencies (*e.g.,*compromise of GlobalSign's private key), which extends to all subscribers and relying parties for Class 2 and Class 3 certificates.

Mr. Mitrakas concluded with a discussion of policy issues. He explained that GlobalSign believes that the legal framework for security should be based on self-regulation. On the side of CAs, requirements include certificate interoperability and branding. On the regulator's side, there may be a requirement for insurance.

Mr. Mitrakas ended his comments with the tentative conclusion that certificates are an integrated industry and that greater co-operation is needed among CAs for the interoperability of certificates.

Lennart Malmstrom, Sweden Post

Mr. Malmstrom explained that Sweden's Postnet offers a variety of CA services, including electronic ID, server certificates, S/Mime certificates, directory services, call centre, and consulting services. His presentation focused on the electronic ID.

The EID card is a smart card based on the SEIS (Secure Electronic Information in Society) standard. It contains three separate key pairs: a pair for identification, a pair for signature and a pair for confidentiality. The key pair for identification allows one to identify oneself. To do so, the other party's site sends a random number which one then signs. The key pair for confidentiality is included in the card because the political outcome of the encryption debate is still uncertain.

The EID supports the use of attribute certificates. These are handled differently from identity certificates because they may have a different lifetime. For example, attribute certificates could indicate one's profession (*e.g.*,doctor), place of employment (*e.g.*,hospital), or assignment (emergency).

PostNet was well-situated to enter the business of offering EIDs because it had issued identification cards for many years and had various procedures in place. PostNet's procedures for the issuance of an EID are as follows. First, a customer must come to the post office with a photo and sign an application. This is to ensure that the EID card is issued to the correct person. Next, the secret keys are generated and put in the card. Public keys are sent to the certification unit that signs them, and the resulting public key certificate is stored in a database or directory and placed in the chip in the EID. If the card is lost, the certificate is revoked.

To demonstrate that EID works, PostNet had 6 000 university students use it to access their exams in the computer system. They could also go to a government Web site and use the EID system to sign their forms for student loans.

Having demonstrated that EID works, the next challenge is to get EID out to the consumer. To do this, PostNet needs a market. To build that market, it is going to companies that need this kind of service and is delivering EID cards to them. The cards can be used for private business within closed user groups, and a number of hospitals have used EID cards to control access to medical information.

Ira Rubenstein, Microsoft

Mr. Rubenstein, of Microsoft, spoke about the online shopping world. He began by identifying two problems with today's online shopping model. First, every time a user visits a Web site, he/she must sign in. This is a problem because people forget their passwords and user names. The second problem is anxiety among users regarding security and privacy. Security is not a key issue for consumers unless they are dealing with an unknown site which might not deliver the goods ordered. Privacy is the key issue and includes issues such as who controls private information and how users can manage and update their information.

Mr. Rubenstein suggested ways to address these problems. First, consumers should be able to sign in once and be recognised many times at many sites. Second, they should have to give demographic information only once, and under a known, defined set of guidelines (*e.g.*,those set out by Trust-e). In addition, they

need a way to use credit cards simply and securely online. Finally, they need to be able to enter shipment information only once and transfer it only as needed.

Mr. Rubenstein next considered the role played by PKI in the online shopping experience and identified two problems: the complexity of PKI technology and the distribution problem. With respect to the former, Mr. Rubenstein recalled Mr. Kent's point, made during the technology primer, that PKI technology and digital certificate technology are too complex for most consumers. Mr. Rubenstein noted that a CPS is much too complex for users who simply want to buy something online; he also pointed out that consumers are not aware that they are responsible for protecting private keys issued to them.

Mr. Rubenstein then described the distribution problem. There is no simple method for ubiquitous delivery of digital certificates to individuals. Browsers are ubiquitous, but digital certificates are not. Credit cards are no doubt distributed in hundreds of millions and browsers are reaching the 100 million mark. However, an installed base of smart-card readers is lacking. Keyboards with installed smart-card slots are just starting to come on the market; most do not have smart-card readers.

Further, who can distribute digital certificates? Government agencies have the reach, but they issue government identification and people may not want to use that ID for online shopping. Alternatively, ISPs might offer certificates as part of the connection service. Finally, portals might offer them, since they want that relationship with users who come to their sites for services/online shopping.

Finally, what provides incentives to distribute certificates? They need to be extremely cheap or free and offered in a way that makes it entirely safe and painless for consumers to use them. One should not have to go to the post office to obtain an ID.

In summary, Mr. Rubenstein argued that what is missing today is a digital certificate that is given to end users. The main use of today's certificates is for server authentication (*i.e.* for SSL, which allows secure transmission of credit card information). Today, most online merchants do not use digital certificates to authenticate customers, because there is no easy way to get certificates to them. At the technology primer, Barb Fox of Microsoft mentioned the digital authentication protocol (hash protocol) which is a password or hash-based authentication protocol used to identify consumers online.

Where is the relationship? Web sites that have already established an end-user base have a relationship, which exists there, not with a third party. Where an entity (*i.e.* rather than trusted third party) has a database of users, the model for online shopping is different from the one that is being discussed here.

2. ELECTRONIC DELIVERY OF PUBLIC SERVICES BY GOVERNMENT

Speakers

- Ari Saapunki, Finnish Population Registry Centre (PRC)
- Lauri Pesonen, SETEC Communications
- Clare Wardle, UK Post Office Legal Services; Jeremy Hilton, JH Consulting
- Katarina De Brisis, Ministry of Labour and Government Administration, Norway
- Yeow Meng Chee, National Computer Board, Singapore

Intervenors

- Michael Baker, Executive Director, Asia-Oceania Electronic Messaging Association
- Casper Bowden, Foundation for Information Policy Research

Ari Saapunki, Finnish Electronic Identification (FINEID)[1]

Mr. Saapunki spoke about the Finnish Electronic Identification (FINEID) project, noting that he sees the future of electronic identification not just as a means of authentication, but as a means of providing a legally binding digital signature. He began by describing the technical side of FINEID, noting that identification, digital signatures and encryption are based on open standards. Chipcards and readers follow ISO standards. FINEID uses X.509 v. 3 certificates and X.500 and lightweight directory access protocol (LDAP) directories. The EID application in the smart card is based on existing *de facto* standards (*e.g.*,FINEID S4-1=PKCS#15). Among the requirements are the use of highly secure environments for key generation and face-to-face identification, which allows the government to guarantee that information in the EID is correct.

Mr. Saapunki next described the general FINEID card object hierarchy. Different kinds of objects can be introduced, including private keys, certificates and trusted CA certificates. He also described the PRC's services, which include a unique ID number, identifying services, certificate revocation lists (CRLs), centralised card manufacturing, open directory service, but no key escrow or key recovery.

Mr. Saapunki mentioned current legislative activity in Finland. The PRC law had been accepted by Parliament and a new law for the EID was going to Parliament. In general, however, there was no need for big changes. The Ministry of Justice supports general laws which set out minimum requirements for electronic signatures, following the EC Directive.

Implementation of the FINEID project is to be carried out in 1999. A group of pilot programmes (six official, 50 unofficial) is under way. Civil servants have been using PRC-CA services in pilot programmes with good results. For example, the Ministry of Agriculture and Forestry (1998, 1999) had direct contact with an EU database, and the Ministry of Social Affairs and Health has a pilot programme in social care and health services. In addition, Parliament and the banking sector have pilot programmes. Involvement in the FINEID project is voluntary, and cards and certificates are only valid for three years. The Finnish police forces will register people. CA and directory services are being outsourced. Finally, there will be a call for tender (open competition) for cards and help desk services.

1. For more information, see www.vaestorekisterikeskus.fi and www.seis.si

The FINEID infrastructure may be used by both the public and private sectors. In the public sector, the FINEID infrastructure provides a basic infrastructure on which new electronic services for citizens can be based. The private sector can offer electronic commerce applications based on FINEID technology (*e.g.*,paying from bank accounts with FINEID technology). The private sector is also offering CA services.

Lauri Pesonen: Security

Ms. Pesonen spoke about smart cards. She first identified three security requirements in open networks: strong authentication, confidentiality and non-repudiation, and then described the difference between symmetric and asymmetric encryption algorithms. She discussed asymmetric algorithms, in which the user encrypts (or signs) with the private key and decrypts (verifies) with the corresponding public key. In particular, digital signature algorithms rely on a private key for signing and a public key for verification of the signature.

Ms. Pesonen then discussed implementation of security services in which each user or process has one or more RSA key pairs. The private RSA key is available only to the owner, or the key user, while the public RSA key is available to all users. The private RSA key is used for a variety of services.

Ms. Pesonen then defined smart cards. A smart card is a card the size of a bank card or credit card, the thickness and flexibility of which is defined by an ISO standard. A "contact" smart card is a smart card that must be inserted into a smart card reader. In a computer's smart card slot (*i.e.* the smart-card reader), there is an I/O connection, and the plate on the front of the smart card makes contact with that I/O line so that information can be transferred to and from the chip in the smart card. Inside the smart card there is a CPU, ROM, RAM, EEPROM (application memory), and a co-processor**.**

Smart cards have several advantages. First, private keys are processed only inside the card. Second, PIN authentication is used for card holder authentication, so that only an authorised person can use the private keys. Third, smart cards are portable. Fourth, they can store a number of private keys and certificates and be used for other (security-sensitive) chip applications (via multi-application cards). Finally, they can be combined with an official visual identification card.

Public key smart cards support various algorithms, including RSA, DSA, ECC, DES, Triple-DES, SHA-1. Elliptic curve cryptography implementations are also on microcontrollers. Finally, public key smart cards have hardware and software security mechanisms that protect against attack.

Ms. Pesonen also discussed RSA smart card performance: *i)* EEPROM: up to 16kb for crypto-controllers; *ii)* hardware-based random number generator; and *iii)* 1024-bit private keys are most commonly used, but up to 2048 bits are supported. Finally, she spoke about the smart card and the PKI. The different parties involved include card manufacturer, card personaliser, card issuer, card holder and CA [and directory and other trusted third party (TTP) services]. There is a secure centralised way of issuing cards.

Ms. Pesonen then turned to smart card system security evaluation, which includes trusting the supplier, doing internal checks, etc., and referred to the use of information technology security evaluation criteria (ITSEC) for security evaluation. The various aspects of the security of smart card systems include physical security, logical security, application security and administrative security (*i.e.* security of production, key management and administrative tasks, if any).

She next identified various standards and open interfaces for interoperability, including ISO standards, PKCS #15 (the specification for digital signature applications on smart cards), PC/SC (the industry standard for the smart card reader interface in computers), and PKCS #11.

Ms. Pesonen concluded with a discussion of future trends. She noted that corporate and private sector issuer schemes are starting to take off and that there is a trend towards national EID card schemes. She also identified a trend towards smart card standardisation, although further work is needed. Finally, she mentioned a trend towards international harmonisation, demand for security evaluations, and use of new algorithms, such as elliptic curves cryptography.

Clare Wardle and Jeremy Hilton: UK Post Office

Mr. Hilton first spoke about the Royal Mail's provision of certification services. He began by introducing the components required for certification services: enabling software, a certification policy, a certification agent and a CA. He then described policy as crucial, as it defines the level of trust at which one works.

In terms of deployment, the UK Post Office's strategy is to serve corporate users first and consumers later. With corporate users, the Post Office can first register the corporation and its top-level employees and next someone in the corporation who can register other employees. Thus, corporate users can have their own internal registration process. This process is more difficult for SMEs as they may not want to undertake internal registration. Mr. Hilton identified CAs as the major expense because they must operate securely and be independently audited.

Mr. Hilton identified three PKI models: the unilateral, the bilateral and the multilateral. The unilateral model simply provides internal authorisation. The bilateral model is used when a company wants to be able to communicate with trading partners. Boeing used this model but then found that its trading partners expected them to continue to provide these services.

After discussing Viacode's objectives, Ms. Wardle explained why the Royal Mail is well-positioned to register people. It has national and international reach and handles around 72 million items of mail a day so that registration is a logical extension of its current operations. It is useful to use outlets whose services are already used to registering people.

Ms. Wardle suggested that the economic model underlying a trusted third party CA is based on network economics: while the first to use a CA do not get much value, value increases as more people use the TTP. Deployment is the key to success in a model based on network economics.

The Post Office must act legally and in accordance with its powers. (British Telecom considered giving free certificates, but that would be illegal because British Telecom is not allowed to take information given for one purpose and use it for another.) In addition, the Post Office must comply with export regulations. Finally, it must manage risk, since it is not just taking on small liabilities.

The UK Post Office's deployment strategy involved identifying its markets and determining what they want. Who are the Post Office's customers? The central government is a possible customer, as a PKI is desirable from the central government's point of view. Indeed, a PKI would help the government comply with data protection requirements, although the government does not want to pay for it. Rather, the UK government hopes to piggyback on what industry is doing anyway. According to Ms. Wardle, however, the UK government has yet to realise that industry does not necessarily want what the government wants and will not be able to set the requirements for a non-governmental PKI. Local government and public bodies are another possible customer base. Local government appears in all sorts of guises, and the Post Office will attack the problem of deployment to this group differently depending on the guise.

Major corporations are a possible customer base. The Post Office can initially seed links through its existing business connections. Thus, it may be able to use this base to enhance deployment. Small and medium-sized enterprises (SMEs) are a possible customer base that would probably not be picked up by

other entities. However, they generally do not want to provide their own help desk support or do their own registration. They could use the Post Office to register or go to trade bodies (who will know who their members are) to complete registration.

Finally, the general public is a possible base, but the questions are, "Who is going to provide these certificates to the public?" and "Will the public pay"? Although the public might pay to submit online tax returns, they probably will expect someone else (*e.g.,*government) to pay for the certificate.

Mr. Hilton next discussed what he described as "the international dilemma": while everyone agrees that cross-certification is a good idea, there is no commercial model. The Universal Postal Union (UPU) is working to get a global model and is trying to obtain bilateral agreements for the registration exercise so that certificates can be issued globally. However, this brings in competition (*e.g.,*Why do CAs want to work together?) Mr. Hilton raised another international issue: the need for equivalence among identification documents. Today, for example, Sweden does not recognise a passport as an identification document. Equivalent levels of documents need to be identified.

Mr. Hilton concluded with the following observations. First, users need to lead the debate. Second, the debate must be about business benefits and not technology. Success depends more on commercial strategy than on technology. Finally, for a PKI effectively to underpin electronic commerce, it needs to provide genuine infrastructure and be truly public.

Katarina De Brisis: Building a PKI for the Norwegian public sector

Ms. De Brisis focused her presentation on Norwegian efforts to build a PKI for the public sector based on voluntary procurement schemes. In particular, she addressed three topics: *i)* electronic government; *ii)* the Public Administrative Network Project; and *iii)* procurement.

Ms. De Brisis explained that Norway will provide a coherent PKI that will be the basis for the provision of public services. The work is being done by the central government in co-operation with local governments.

As part of its effort to establish a PKI, Norway began the Public Administration Network (PAN) Project in 1996. Characteristics of the PAN project include user-driven development and exploitation of market mechanisms. As Ms. De Brisis explained, framework agreements have been developed as part of the project between public sector organisations and TTP service suppliers in Norway. The agreements are based on "a common requirements specification" which defines the standards for the TTP services used by public sector organisations that purchase under the framework agreement. Use of the framework agreement by the public sector is voluntary. Thus, the PAN project is a voluntary procurement scheme to establish framework agreements which will facilitate the establishment of a PKI which can be used as the basis for the provision of public services. Voluntary procurement agreements have been established in several areas and cover local and central government.

Finally, with regard to procurement, two new procurement areas were set out in 1998. One covered EDI and electronic forms and the other TTP services and message security (digital signature and message encryption, smart card readers and smart cards). However, as Ms. De Brisis noted, the PKI scheme is not to be used for national security documents.

Agreements have been reached for TTP services for the issuance of general identification certification, not for identification of citizens. Ms. De Brisis noted that the main requirements (for products and services rendered) were modified SIES standards. (The standards were modified because Norway was not requesting visual identity cards and because the government wanted digital signature encryption keys stored in a smart card.) Requirements included three key pairs and a self-assessment test project to define

requirements for the interoperability of devices. The agreements also set out TTP service providers' liabilities with special conditions for third-party providers. These are liable for breach of trust in the certificate (*e.g.*,certificates wrongly issued, with incorrect content, or wrongly revoked). The agreements were only concluded for one year, so that there were low caps on liability. Finally, if damage (breach of trust) occurs at a cross-certified TTP, the customer's TTP is liable for the damage (but is not liable in the case of increased liability). TTP suppliers are developing a cross-certification scheme. Three suppliers of TTP services are developing bilateral agreements and a common certification policy.

Ms. De Brisis then discussed the proposed common rules for naming and identifying certificate users and certificate content. She described four types of certification: organisation certification (legal person); personal certification (civil servant); role certification (units/positions); and profession certification (health professionals, barristers, etc.). Unique identifiers are used for organisations.

Ms. De Brisis identified the following PKI-based applications: electronic administrative procedures; electronic commerce (public procurement); and electronic services to citizens/firms (tax returns online, health network, etc.).

With regard to the current legal situation in Norway, Ms. De Brisis said that the Digital Signature Task Force has made a report to the Information Security Council, which has made recommendations to the Ministry of Industry and Trade. There is an upcoming White Paper on electronic commerce, and a law survey project is under way. Norway is preparing implementation of the EC Directive on electronic signatures. Finally, a new task force has been designated by the Ministry of Industry and Trade.

Dr. Yeow Meng Chee: Singapore's work on security

Dr. Chee began by describing some recent milestones in electronic commerce in Singapore. Singapore's E-Commerce Policy Framework was released in December 1997; it contained a set of public and private sector recommendations to the government. Included was a recommendation to establish a PKI and to enact an Electronic Transactions Act. The PKI was implemented in July 1997. The Electronic Transactions Act was promulgated in July 1998 and provides, among other things, for the "acceptance of electronic signatures" and for limitations on liability for licensed CAs. Next, in September 1998, Singapore published an E-Commerce Masterplan.

Singapore is involved in international efforts in the areas of cross-certification and harmonisation of cross-border policies. Recognising cross-certification as one mechanism for interoperability, Singapore has an implementation arrangement with Canada. In addition, Singapore and Canada will co-chair the new APEC task force (*i.e.* the authentication task force), which will be set up to address cross-certification issues. Singapore is also involved in work towards the harmonisation of cross-border policies through international bodies such as UNCITRAL.

The implementation of a PKI in Singapore is part of a broader effort to provide traditional public services online (PSO). Mr. Chee identified several that are now available. These included the Central Provident Fund (CPF), the Integrated Land Information Service, the Electronic Survey System, electronic development applications, cyberbanking, online share trading, and MINDEF Internet Procurement System (MIPS). The CPF is similar to a retirement savings scheme; its beneficiaries can download up-to-date statements, and employers now submit employee contributions over the Internet. The Integrated Land Information Service integrates map and texture and sells the information to land developers, architects and lawyers. Users can download digital maps with land information from the Registry of Titles, Land Office and Survey Department and pay by cash card or giro. The Electronic Survey System allows respondents to retrieve survey forms and send completed forms back in encrypted form. An electronic development

application enables architects to submit their plans for approval; it relies on an artificial intelligence engine in conjunction with security to ensure that building plans are built to specification. Much work is being done in the area of cyberbanking. Three major banks are offering banking over the Internet; some offer portfolio management but not share trading. Online share trading is available, with 24-hour access, live stock exchange quotes, and online trading. Finally, MIPS allows trading partners to view invitations, submit quotes, receive purchase orders, submit invoices and view payment status. The purpose of authentication in this context is to identify trading partners and know with whom one is trading.

Mr. Chee offered three conclusions. First, the next step is to combine security with rights management technology. Second, it is important to go beyond technical problems to consider the business, policy and legislative issues. Finally, co-operation between the government and the private sector is necessary. Mr. Chee noted that he looks forward to a PKI that is interoperable worldwide.[2]

Michael Baker, Intervenor

Mr. Baker, taking the SME perspective, asked the speakers, "If you are going to trade with Asia, how are you going to be high-tech in your own country and deal in a low-tech way with other parts of the world?" There is, he noted, a wide range of technical capabilities in the Asian region. Japan and Singapore are the equivalent of, or better than, Europe and the United States with respect to technological innovation. However, other countries are less advanced (*e.g.*,one Asian telecom rolled out an EDI system on the X.400 system, and in another country in the region, some people keep money under their mattresses because they do not trust the banks). There is both a technology issue and a trust issue in some countries.

Response

Ms. Wardle of the UK Post Office responded that the United Kingdom cannot provide the infrastructure around the world. Individual countries have to deal with that. However, the United Kingdom feels that there are ways to get people to use these services once they are online.

Casper Bowden, Intervenor

Mr. Bowden took a consumer/user perspective. His main point was that a hybrid of encryption and authentication might provide a way for users or consumers to protect their privacy. He first suggested looking at the range of technology-driven information issues, including encryption as well as authentication. With respect to encryption, Mr. Bowden noted that he is an active participant in the UK debate on cryptography policy and that the Cabinet office has decided that no licensing system that government might introduce will have any link to key escrow.

Mr. Bowden then noted a connection between authentication and data protection (encryption). He drew attention to the relation between the online shopping environment to which Mr. Rubenstein referred and the strong general-purpose ID. How do they relate to each other? There are privacy risks/concerns when transactions are associated with a digital ID. For example, there is concern about an audit trail, since a digital signature is different from a signature on paper and poses a greater threat to privacy. Similarly, an ID or name certificate is different from an attribute certificate and also poses a greater threat to privacy.

---

2. For more information, see www.cca.gov.sg/, www.ec.gov.sg/, www.ncb.gov.sg/

However, Mr. Bowden felt that a hybrid of encryption and authentication might allow users or consumers to manage a large number of randomly generated identities so that they could protect their privacy in ways impossible today unless they are very diligent.

Mr. Bowden left the speakers with two questions. *i)* Is there a future for general-purpose ID certificates in browsers on the Internet, and if so, how will they be achieved? and *ii)* If there is a future for general purpose ID certificates, what degree of anonymity should and would consumers routinely be given?

Response

Ms. De Brisis of Norway responded that there is no future for general purposes ID certificates. She does not envision a single certificate. If people want digital certificates, they will have to have more than one. There will not be one identification certificate for every purpose. Even now, when one uses a Web page, one gives one's user name and password, so that audit trails already exist.

Another panellist responded that people will use their general purpose ID with the government and then use it indirectly, to get certificates, for other purposes.

Another respondent noted that anonymous payments are possible when using a stored value card. The Common Electronic Purse Standards are also a possibility for an anonymous Internet payment standard. When there is a global standard for electronic cash, there will be a standard for small or anonymous payments and a way to make anonymous payments.

To take Michael Baker's question a little bit further, one might ask to what extent law should drive technology or technology drive law? What if policy makers demand certain technologies and not everyone can afford or access them?

Neither law nor technology should drive the other. Law may follow if things are out of order, but law should not lead, yet some countries are starting to put technology into their laws (*e.g.*,the Philippines quotes EDIfact standards in its law). There is also a danger of that in the Directive on electronic signatures. It is necessary to look at what people want, need, etc. It is equally misconceived when laws assume a hierarchical CA.

Ms. De Brisis then observed that it is not clear that there is a need for new laws. Rather, one should look at the purpose behind old laws. What was the original intent of the regulation? Did the original legislation require paper and handwritten signatures? She suggested that either a handwritten or an electronic signature could achieve the intent of the legislation. She added that law should be as technology-independent as possible and that law, or encouragement from public authorities, might play a role in the lack of trust problem.

Another speaker said that government should guide, not legislate unless it is prepared to change legislation on the basis of experience. A lot has been said about government-sponsored projects. A policy-based role rather than legislative role could address access issues by funding projects (*e.g.*,public kiosks) so that it is not necessary to own a device in order to access the Internet.

Ms. Wardle noted that the United Kingdom has backed away from government-imposed regulation and that governments can encourage self-regulation efforts and ensure that consumer rights will be protected.

Question

Noting that the speakers have discussed PKI infrastructures in different parts of the world, each of which has its own rate of technology adoption, a listener asked, "Do you have individual/regional perspectives on the cultural perspective that will impact rate of adoption?"

Responses

Mr. Saapunki said that Finland is trying to create a global PKI solution. Ms. De Brisis suggested that one difference is that the technology adoption rate varies from country to country and another is that there is other electronic infrastructure in place in various countries. There are differences between Nordic countries and European countries. The Nordic countries have a unique ID number for individuals and national central registers already hold sensitive information, that is, they are already trusted parties. Their electronic infrastructure helps them support emerging PKIs. That might not be the case in Europe and the United States.

Another speaker pointed out that citizens' behaviour also differs, and harmonisation could take some time. However, all have in common the fact of transactions over open networks. That lends enough similarity to lead to interoperability.

Mr. Hilton then spoke of an education issue. Gaining acceptance by the next generation, so that it is prepared to embrace this technology, could take a long time.

Ms. De Brisis mentioned the number of people with telephones in African countries. She added that there are different kinds of identification documents. Identification cards, for example, are acceptable in some places, but not in others, such as the United Kingdom.

Mr. Chee distinguished slower rates of adoption of technology due to poverty from slower rates of adoption due to cultural issues. He suggested that cultural differences surface particularly for e-commerce in general. For example, Asians are not very accustomed to mail order or buying from catalogues. A slower rate of technology adoption is a secondary effect of that phenomenon.

Yet another speaker noted that mobile telephone networks can be used and may be an appropriate medium for delivering technologies and subsequent applications.

John Dryden, OECD

Mr. Dryden was struck by the degree of consensus on objectives and possible policy means of achieving those objectives. He posed two questions. First, what initiatives are needed at the international level to facilitate the adoption of electronic commerce in light of the diversity of levels of development and approaches? Second, what kind of institutions (*e.g.*,UNCITRAL) does the panel think could be a vehicle for taking those initiatives?

Response

Ms. De Brisis said that initiatives must be taken in standards and that the standardisation process must be quick and at industry level. If a forum were provided for industry to convene and agree on standards without too many complications, it would probably help a lot.

Jeremy Hilton argued that demonstrable interoperability is needed so that standards are pragmatic ones. Vendors need to collaborate. In the international arena, vendors should be encouraged to demonstrate interoperability.

Clare Wardle turned to tax issues, to maintain that some of the bizarre complexities with respect to services provided over the Internet needed to be sorted out. There is also concern about import and export controls, as it may take months to get permits to export something to a country where the thing is readily available. An international initiative would be very useful. In addition, encryption should be removed from the Waasenaar agreement and barriers that prevent use of these technologies should be removed.

Another participant added that legal interoperability is also needed. Certificate authorities would do well if they co-operated. Perhaps legislators might introduce legislation that facilitates co-operation. For example, under the Directive on electronic signatures, there are four statutory liabilities for unlicensed CAs which do not necessarily exist under similar laws (*e.g.*,those of California in the United States). So, there may be different standards that might, in future, inhibit development of CAs and CA services.

In response to another question about whether panellists see problems with non-repudiation because of where the keys are being generated in some systems, Mr. Hilton responded that he did. Defining a policy is very important. Mechanisms are needed for key generation and implementation of software that does key generation (*e.g.*,it does it only once and does not copy the private key while generating). Protocols must demonstrate that when one has a certificate, it is valid. Finally, experience in the courts will show how much trust one can put into the system. Ms. Wardle agreed that the issue was signature keys.

Session IV: Organisation-to-Organisation Transactions

Moderator

- Peter Ferguson, Industry Canada

Chairman's welcome

Mr. Reaburn began with a short privacy anecdote. He said that in New South Wales, Australia, a dangerous criminal escaped from prison by trading places with a person who came to visit him. As a result, the state introduced a new regime for visitors to prisons. It announced that it would take the fingerprints of visitors on the way in and the way out of the prison. There was an immediate outcry from families of inmates who were concerned about their privacy. The company that was hired to implement the system responded by assuring the families that the company was not going to store the fingerprints but just a string of numbers.

The Chairman then stressed that WPISP is concerned with information security and privacy. While its focus is on information security, the need to keep the context in mind and take account of privacy must be taken into account.

Peter Ferguson

Mr. Ferguson opened by saying that the focus of the session was public policy and legal issues rather than technical details. Mr. Ferguson noted that there would be two panels, the first panel focusing on business-to-business transactions and the second on electronic authentication in government transactions.

1. BUSINESS-TO-BUSINESS TRANSACTIONS

Speakers

- Bhaskar Kakulavarapu, Manager, Advanced Technology, Lear Corporation (ANX)
- Bill Tiga Tita, G77 Chamber of Commerce and Industry for Developing Countries Network
- Ken Fitzpatrick, Business Line Manager, PKI Security, IBM

Bashkar Kakulavarapu: ANX

Mr. Kakulavarapu's topic was the current Automotive Network eXchange (ANX) architecture and the status of ANX. First, he presented the Automotive Industry Action Group (AIAG) of 1 500 automotive companies. Its objectives include providing an open forum in which members co-operate and communicate to improve business processes and practices, to address existing and emerging common issues and to apply new and current technology to increase the industry's efficiency. The development of ANX is a project of the AIAG.

The aim of the ANX architecture is to provide an end-to-end network that will serve as a business Internet. The AIAG invited telephone companies to participate and, under Bellcore (at that time), developed an architecture over a period of three years.

A variety of pilot projects have been completed or are under way. In Germany, a pilot project has been completed, in the United Kingdom and in France, pilots are being carried out, and discussions are under way in South America. During the first complete successful ANX pilot, Ameritech, ATT and Bell Canada served as certified service providers (100% guaranteed) and there were over 100 fully subscribed trading partner connections. While companies will continue to use the Internet for lower-end applications, most applications will move to ANX in the future.

Mr. Kakulavarapu next outlined the components of ANX's security vision. First, ANX seeks agreement on a set of basic principles designed to meet global business requirements. Second, ANX envisions global companies supporting a common strategy and speaking with a single voice in all national associations in order to minimise national politics in dealing with authentication issues. In addition, ANX envisions formal agreements to share intellectual property and pilot experience so that ANX trading partners can share experience with entities around the globe. Finally, ANX envisions seamless interaction with external PKIs.

Mr. Kakulavarapu then described the ANX business model for its authentication architecture. The business model provides that ANX will authenticate user access, providing privacy and verification; provide data integrity during transit; provide non-repudiation and prevent denial of service; be user-friendly, establishing ease of use for all business processes; secure corporate data; ensure high security infrastructure; scale to millions and have high availability; provide support for the global business environment.

Mr. Kakulavarapu then mentioned a variety of challenges. First, the CA's legal responsibilities and jurisdiction must be defined. Second, CA accountability for protecting, verifying and authenticating end user certificates must be established. Third, legal requirements for archiving and retrieval of old certificates must be established. Fourth, insurance and liability protection for the business entity, end user, and CA must be set. Finally, each CA must accept and abide by cost models developed by the ANX Strategic Task Force and Overseer.

Mr. Kakulavarapu then discussed ANX security requirements. ANX is based on IPSec (Internet Protocol Security) products. It relies on IPSec End Device Certificates only, uses IPSec Gateways (VPN concept) and has an IPSec dial-up client (for laptops and desktops). Other requirements include a CA policy, an ANX PKI, a certification profile, and CA practices.

Mr. Kakulavarapu then presented three technical models for the ANX architecture. First, there is the self-signed root certificate, the advantages of which are that it raises no interoperability issues and is a simple architecture. Its disadvantage is that it is a CA-based business model, and it is difficult to bring in new CAs. Indeed, Mr. Kakulavarapu noted that a global root is impractical for the automobile industry.

Second is a model with multiple CAs and cross certification. In this system, each CA has a self-signed root certificate, there is a policy mapping between CAs, and each CA certifies the others as a trusted party. The disadvantages are that the number of cross certificate pairs to manage is (N-1), and that it is difficult to remove a CA.

The third alternative is called the "bridge" CA, and in this model, a bridge CA certifies each CA. This model has several advantages. First, the number of cross-certificate pairs to manage is equal only to the number of CAs. In addition, the model has good operational scaling, that is, if there are N CAs within a bridged ANX PKI, there are only N cross-certificate pairs with external PKIs. Finally, it is simple to remove a bridge CA.

Next, Mr. Kakulavarapu identified several challenges. First, there is a development challenge because the technology is not yet well understood. Second, interoperability is a challenge because it requires tools to load different certificates, and different standards are being implemented. Other challenges include achieving interoperability with external PKIs and allocating liability.

Mr. Kakulavarapu said that ANX will implement authentication based on digital certificates, initially using IPSec devices (*i.e.* IPSec gateways and client dial-ups).

Mr. Kakulavarapu's final comments focused on future global policies. These must support various business models; there must be common law to avoid ambiguity; there must be tracking and auditing requirements and policies; there must be archival capability and backward compatibility of technology (*i.e.* ten years later it must be possible to get a certificate if it is needed); there must be legal protection for all entities involved; and the cost of doing business securely must be reduced.

Bill Tiga Tita: Worldchambers Consortium[3]

In describing the activities of the G77[4] Chamber Network, Mr. Tiga Tita began by alluding to the importance of trust and confidence as distinct from security and authentication. He identified several potential means of developing trust and confidence, including regulation of individual behaviour, establishment of codes of conduct (*i.e.* "we will behave like gentlemen"), insurance and technology (*i.e.* tools). Mr. Tiga Tita explained that regulation of the behaviour of individuals is insufficient to establish trust and suggested that insurance does not solve the trust problem either. Indeed, he compared insurance to a premarital contract: it is not sufficient to solve the trust problem that causes the breakdown of a marriage.

3. For more information, see www.trustinfo.net and www.trustinfo.org .

4. The G77 is a group of 133 countries.

Mr. Tiga Tita then suggested that trust is needed before, during and after the commercial activity. During the "contact" stage, parties may want to obtain certain information (*e.g.*,who the contact is and what the contact does). In this initial stage, a system of proofs is the main requirement of an authentication system. In the second, negotiation stage, signature certification is needed. Finally, in the delivery stage, customer satisfaction is the main requirement.

Mr. Tiga Tita then pointed out some ways in which the Internet differs from other media. First, there is a lack of objective information. Second, there is an abundance of noise. And, third, the Internet is teeming with lies, rumours and manipulation. He then offered a recipe for "confidence cake", the ingredients of which included use of proofs (*e.g.*,users can ask TTPs to provide references); labelling and self-discipline by TTPs; establishment of a code of practice; and validation.

Mr. Tiga Tita then discussed two aspects of validating information, and noted that letters of introduction and a seal of approval could be combined to establish trust and confidence. The former would serve as proofs, establishing one's qualifications in the "contact" stage of a transaction, while the latter would serve as a quality certification (*e.g.*,in the self-discipline context, a label represents adherence to some minimum code of conduct). This is not new; the idea is simply to encourage information validation so that information can be trusted.

Ken Fitzpatrick: IBM

Mr. Fitzpatrick's main point was that a rigorous registration process is the foundation for trusted applications. He began by recalling that security is a primary concern and that trust and confidence in the people with whom one does business is also a concern. He pointed out that no-one has a passport online because passports need to be issued by an authority and no-one has been recognised as an authority to issue passports online. In fact, if there were such an authority, people would question its validity.

For this reason, Mr. Fitzpatrick identified the challenge as building trust into electronic business. This requires the ability to identify and authenticate those with whom one does business and also involves enabling trusted e-business with PKI. He then observed that the first rule of business is know your customer, but the first rule of the Internet is that you cannot know your customer.

Mr. Fitzpatrick went on to suggest that there is a lot of "hype" about authentication because business drivers and enabling technologies are converging. All countries and businesses want to take advantage of electronic media and are seeking ways to build trust and confidence into these processes and technologies so that they can conduct business in the electronic world.

Mr. Fitzpatrick suggested that when talking about identities and authentication, one immediately brings in issues of privacy, data integrity, confidentiality and non-repudiation. He identified six areas of importance: security management (which includes trust and confidence as well as security); non-repudiation (the legal aspect); data integrity; privacy; access control; and authentication (*i.e.* identifying users and entities).

Mr. Fitzpatrick then presented three authentication case studies: Datakom Austria, Banco Mercantil, and Equifax.

Datakom Austria is a subsidiary of Post and Telecom Austria which has established itself as a TTP. Mr. Fitzpatrick asks, "What gives Datakom Austria the right to authenticate people?" They have designed and implemented technologies that allow them to be a registration authority, and they offer multiple PKI and TTP services. The number one challenge to Datakom Austria is how to register, authenticate and identify the individual, given that the company's premise is never to trust anyone, including your own people (in the United States, 72% of all electronic violations take place within the company). Datakom

Austria faces the further challenge of how to register, authenticate and identify individuals so that these actions will hold up in a court of law. This requires time stamping, audit logs and other precautions. Indeed, everything that is required in the real world is also required in the digital world. The major differences stem from the need to prevent tampering that compromises or modifies information.

Banco Mercantil is a corporate banking firm in Venezuela that does business-to-business transactions. Mr. Fitzpatrick explained how corporate customers get digital certificates.

In the traditional world, Equifax is a TTP in the banking industry (*e.g.* it does financial creditworthiness checks) and it does the same thing in the electronic world. Equifax issues electronic authentication (in the form of digital certificates) to authenticate people.

Mr. Fitzpatrick suggested that a rigorous registration process is the foundation for trusted applications. If the registration process is not rigorous and the technology will not hold up under the law, nothing else matters. With regard to the registration application, before a user gets access to a Web site some kind of credential must be provided. Registration is the process used to authenticate an individual and in the digital world, it must be electronic because a manual process would expose the user to fraud.

Mr. Fitzpatrick then asked the questions, "Who should deal with the issues, policies and standards in a global world" and "When does government get involved to help set policy?"

Mr. Fitzpatrick concluded that there are several types of certification: digital signing, encryption signing, and authentication. The most robust authentication is achieved when it can be proven beyond reasonable doubt in a court of law. Below that, there may be different levels of certification.

Question and answer period

Mr. Bowden spoke from the perspective of consumer protection. He asked about subject access, noting that subject access is an important principle in the data protection framework in Europe, and wanted to know if this is an area in which mainstream companies are active.

In response, Mr. Fitzpatrick said that we would know that we have established subject access, and asset control in general, when control of information is handled by the owner of the information. Today, some technologies can manipulate information without knowledge of the owner.

Mr. Fitzpatrick added that, as a supplier and vendor of technology, IBM must work with other vendors to push open standards. If something happens in Europe in the banking industry or in the deregulation of telecoms, it is feared that interoperability issues will be barriers. Mr. Fitzpatrick stated that the Internet Engineering Task Force (IETF) has done a great deal to help to establish PKIX protocols and said that the adoption rate is helping IBM to move faster.

A representative of Telecom Italia said that Telecom Italia manages an ISP function inside the company. It uses electronic commerce certificates to manage all activities on its intranets (and can therefore control information). It is building a metadirectory capable of matching users and services in a dynamic way by associating an object database with LDAP.

Telecom Italia serves as its own CA. All Telecom Italia authentication systems are integrated with infrastructure services (e-mail, navigation, integration with legacy). With regard to the CA and registration authority (RA) environments, Telecom Italia has developed a specific service for certification named "VillageTrust". This has been a commercial service since last year. Telecom Italia focuses on the RA as a

reference point for building the PKI, because it is convinced that an Internet trial would be useful to test TTP functionality. Telecom Italia relies in part on auditing to control activities.

In the privacy area, Telecom Italia has focused on knowledge management activities as a way to discharge its data ownership responsibility. It sees a good model of e-mail as very important. E-mail has three aspects: classic e-mail, certified e-mail via certificate, and use-structured certificate e-mail for EDI. There is also a cultural challenge, in that new concepts of authentication need to match new business models.

In response, Mr. Fitzpatrick elaborated on the Equifax/Home Depot case study. Equifax is a TTP working for two parties: Home Depot and IBM. IBM, like Home Depot, has decided that it does not want to authenticate people nor does it want disintermediation between itself and its customers. (There are service providers in the ANX world which are establishing themselves as, or are being recognised as, a certificate authority. Telecom Italia similarly serves as its own CA. If a company wants to be in that business, the technologies are in place to do so.)

Equifax is in the business of authenticating people. It acts as a registration authority, and, using IBM products, registration is completed by a certified RA (the RA's qualifications have to be certified for the RA to be a certified RA) in a highly secure environment. IBM also enabled Equifax to run multiple CAs off a single RA or a single CA off multiple RAs.

Equifax chose an IBM product because IBM's registration process ties into a company's existing business policies and practices, including privacy practices. Equifax, for example, needed isolation and protection of information, and IBM's vault technology provides that. The vault technology essentially stores encrypted data in individual "vaults". Mr. Fitzpatrick explained the motivation for the development of the vault technology with the following example. Assume that Home Depot is concerned about its competitors gaining access to its data. Home Depot might be concerned that Equifax, acting as an RA for both Home Depot and Home Depot's competitors, would enable Home Depot's competitors to access Home Depot's data. In order to respond to Home Depot's concerns, Equifax wants a highly secure, trusted environment. IBM's vault technology was designed to provide this.

The vault technology addresses several issues, including the competitive nature of business and risk management, and CFOs (chief financial officers) are concerned with protecting data, dollars or high-value transactions. The approach used by the vault technology is to give customers "safe deposit boxes" which cannot be unlocked without both a private key and a bank key. For security, transactions are end-to-end encrypted at all times and data is kept in a vault. Data is always encrypted with public and private keys at both ends, and the end user uses a private key to communicate with others.

In response to Ms. Peters' question about the degree of security available, Mr. Fitzpatrick noted that DES, key recovery, and integrated vault technology are available in IBM products. In addition, IBM is working with Intel on CDSA (common data security architecture) which offers "plug and play" services for cryptographic services (*i.e.* one can snap in one's own encryption algorithms).

In response to a question about IBM's position with regard to US laws on export control, Mr. Fitzpatrick explained that IBM's position is that government has not moved fast enough. IBM is not happy with the speed at which it is getting approval for exports of strong encryption. However, once IBM implements key recovery, there will be no more export restrictions. Therefore, IBM is accelerating its work to make key recovery available so that it will no longer face this problem.

2. ELECTRONIC AUTHENTICATION IN GOVERNMENT TRANSACTIONS

Speakers

- John Weigelt, Senior Technical Advisor, PKI Task Force, Canada
- Richard Guida, Chair, US Federal PKI Steering Committee; member of the Government Information Technology Services (GITS) Board
- Lionel Vodzislawsky, Project on electronic declarations for VAT and customs, Ministry of Economy, Finance and Industry, France

Intervenors

- Jacques Pantin, Chief Executive Officer, Certplus (a certification authority in France with France Telecom)
- Robert Fisher, Manager, PricewaterhouseCoopers Technology Consultants
- Peter Stokes, Deputy Chief Operations Officer, Tradelink Electronic Commerce, Hong Kong, China

John Weigelt, PKI Task Force, Canada[5]

Mr. Weigelt spoke about the government's PKI. He recalled that Canada began initial R&D in 1993 and a few years later, undertook risk assessments and looked at the requirements for support of a government PKI as an enterprise. The final COTS (commercial off-the-shelf) product is due in the third quarter of 1999. Canada has taken a top-down, "field of dreams" approach: the government is building the infrastructure and hopes the applications will come.

In terms of the legal requirements that affect the PKI, Mr. Weigelt said that a bill is pending that will remove the paper bias in existing legislation. The bill also recognises electronic signatures and "secure" electronic signatures, and it establishes rebuttable evidentiary standards.

On 28 May 1999, Canada's PKI policy was approved by the Treasury Board. It has several elements. First, it includes subscriber agreements, with a long form for business and a short form for consumers. In addition, there is an employee use policy. There is also a sample cross-certification agreement, and Mr. Weigelt remarked that the Task Force foresees widespread cross-certification within government and with trading partners. The policy also includes "contracting out" guidelines, which allows "contracting out" certificate services. This is similar to the certificate utility described by Warwick Ford during the technology primer. Certificate policies define the obligations of CAs and include four levels of assurance for signature and confidentiality keys.

Mr. Weigelt noted that the PKI infrastructure is designed for the normal business transactions conducted by the government and is not for classified information. He noted that over 100 applications will use the PKI and identified key projects, including electronic services and secure messaging. One electronic services application made it possible to do 850 000 applications for spectrum allocation electronically, but Mr. Weigelt identified secure messaging (*e.g.*,at ministerial level) as the "killer application" for

5. For more information, see www.cio-dpi.gc.ca.

government. He also discussed four applications that illustrate the use of secure electronic service delivery (secure ESD): employment insurance; record of employment; end-to-end procurement; and corporate income tax.

Mr. Weigelt then identified three types of transactions: secured publication of information; form submission (*e.g.*,employment insurance forms); and e-commerce (*e.g.*,payment).

Mr. Weigelt next turned to a variety of issues that Canada is addressing in implementing its PKI. First is the problem of assurance levels and what qualifies as an appropriate level of assurance for certificates and applications. In addition, it is considering whether there should be one or multiple levels of assurance.

Second, Canada is considering whether or not to outsource the CA function. There is trust in the Canadian government, and the government is addressing the problem of how to instil trust in CA services.

Third, the government is considering the problem of multiple certificates. This issue is not yet well understood. Canada is considering an ID certificate and a certificate with multiple attributes. Ease of use is one concern, as the government wants the population to be able to use the solution adopted easily. In a related effort, it is trying to identify the minimum amount of information required in a certificate.

Fourth, the government is considering issues that arise from identification of certificate "holders". For example, if the Canadian Department of Corrections issues certificates to parolees and the certificate identifies the issuer, people will know when a person is a parolee. Identification of certification "holders" might facilitate discrimination.

Fifth, the Canadian government is considering the issue of fees. While it may charge minimal fees to industry, it is trying to avoid fees altogether.

Sixth, the government is considering various registration models. The "big bang" approach would involve registration of masses of people using kiosks. Another approach would be to register people with continuing relationships. In addition to the question of how, initially, to register people, the government is considering how levels of assurance will change over time. Will one's level of assurance increase over time? For example, if a low assurance certificate is issued initially and is used over a significant period (*e.g.*,ten years) will the assurance level increase?

Finally, the Canadian government is considering various architecture models.

Having identified the range of issues being addressed, Mr. Weigelt indicated that PKI is 80% policy and 20% technology. He noted the need for certificate policies, certification practice statements and cross-certification guidelines and emphasised that legal, policy, operations, application and technical experts are essential for success. Indeed, Mr. Weigelt noted that from the various areas involved 1.5 person years went into developing Canada's CA policy. Mr. Weigelt also stressed that applications provide the business case for the PKI and that Canada will need "buy in" to get the project to work.

In conclusion, Mr. Weigelt identified three challenges for the PKI Task Force as it moves ahead. One is providing certificates for industry and citizens. Second, it will seek cross-certification with external PKIs (*e.g.*,with ANX). Indeed, it hopes to have criteria for cross-certification by the end of the year. The third and final challenge is the development of a management infrastructure. Currently, Canada has an identity-based PKI. The next step is to include attributes and to have attribute authorities that are tightly linked to the PKI.

Richard Guida, Chair, US Federal PKI Steering Committee[6]

Mr. Guida spoke about US federal agencies and electronic transactions. He began his presentation by commenting that the Federal PKI Steering Committee is trying to learn from those who have deployed, and are deploying, public key technology effectively. He noted that, unlike the Canadian government, which has taken a top-down approach to the development of its PKI, the United States is taking a bottom-up approach; that is, agencies are using public key technology in agency-specific applications without central direction.

Mr. Guida identified four types of electronic transactions involving US federal agencies: intra-agency, interagency, agency to trading partner, and agency to public. He then listed several electronic transaction drivers, including long-term cost savings; trading partner practices (*e.g.*,practices of banks); public expectations (*e.g.*,the public wants 24-hour service and does not want to stand in line); federal statutes (*e.g.*,the Government Paperwork Elimination Act) and federal policies; and international competition.

Mr. Guida then described the GPEA in greater detail. Enacted in October 1998, GPEA focuses on transactions with federal agencies. The law is technology-neutral, discusses electronic, but not exclusively digital, signatures, and gives electronic signatures full legal effect. He pointed out that technological neutrality does not mean that "all technology is born equivalent", but rather that, when considering the kind of technology to deploy for a particular application, one must think about the requirements of the application. Mr. Guida noted that US law focuses on providing an opportunity for the market to decide which are the right technologies for particular applications.

Mr. Guida then outlined the timeline for implementation of the GPEA. Draft Office of Management and budget Guidance has already come out, and final guidance is due by April 2000. Compliance is required by October 2003. Thus, federal agencies need to accept electronic forms over the Internet by 2003.

Next, Mr. Guida discussed several intra-agency PKI projects. Originally known as pilots, these projects have evolved to a more robust state. Mr. Guida mentioned projects involving the Department of Defense (DoD), the Federal Aviation Administration (FAA), the Federal Deposit Insurance Corporation (FDIC), the National Aeronautics and Space Administration (NASA), and the Department of Energy (DOE). The DoD, for example, currently has over 10 000 high-assurance certificates on smart cards (*i.e.* hardware-tokenised) and will have 4 million by 2002. DoD certificates are identity-based certificates being used to secure the infrastructure. The FAA has about 1 000 certificates and will have 20 000 by the year 2000. The FAA currently uses software, but is likely to migrate to smart cards. All FDIC employees are PKI-enabled, but not everyone has certificates. Currently, 1 000 certificates have been issued, and eventually there will be 7 000.

Mr. Guida continued with a discussion of three trust models for interoperability. The first was peer-to-peer cross-certification, also known as bridge certification. The second was the validation authority approach, in which there is an entity to whom one would go to validate that a certificate has not been revoked; that entity is a "trust anchor." Finally, there is the trust list, which is a "browser model"; it has appeal because everyone has a browser. However, this model is difficult to manage because it is very decentralised.

Mr. Guida then described the federal PKI approach. First, an overall federal policy authority is being established. Second, the Steering Committee has decided that the federal PKI will support all three approaches to interoperability, and the marketplace will decide among them. In the short term, however, it is necessary to facilitate interoperability. To this end, the United States is developing a bridge CA using

6. For more information, see www.gits-sec.treas.gov.

COTS. The National Technology Information Service (NTIS)[7] is taking the technical lead along with the National Security Agency (NSA), the National Institute of Standards and Technology (NIST) and the General Services Administration (GSA). Four levels of assurance will be offered, emulating Canada's certificate policy. A prototype is due late in 1999,[8] and a production version is due early in 2000.[9] Directory issues will be dealt with in parallel with interoperability issues, and ACES (Access Certificates for Electronic Services) will be used for transactions with the public.

ACES is the principal model for doing business with the public. It is a GSA effort to provide no-cost certificates to the public. Certificates and information provided by subscribers in order to obtain certificates are subject to United States Privacy Act requirements and are for business with the federal agencies (or federally sponsored programmes) only. ACES certificates can be obtained via online registration or in-person application. Once the applicant's information is vetted, a one-time PIN is mailed (out of band) to the applicant, who generates his or her own key pair, then connects to the ACES CA using SSL and passes on the public key and the PIN to get the certificate. Agencies are then billed per use or per certificate. A request for proposals for ACES was issued in January 1999 and bids were received in April 1999. Multiple awards are planned (bidders must meet the low price) and awards will be made late 1999.[10]

In conclusion, Mr. Guida mentioned legal uncertainty as an obstacle. In particular, he pointed out that owing to the absence of case law involving the use of electronic signature, large uncertainties accompany their use. Attorneys work hard to minimise exposure to risk and are uncomfortable dealing with situations in which uncertainties are so large. However, Mr. Guida observed that in the realm of jurisprudence, uncertainties are abundant. Indeed, there are enormous uncertainties in proving anything, and he expressed confidence that it will not be any harder to prove the validity of an electronic signature (*e.g.*,by calling expert witnesses to testify about cryptographic methods) than it is to explain to a judge or jury other complex technologies which are carried out routinely (*e.g.*,DNA evidence, environmental data, radioactivity, the Internal Revenue Code, etc.). Indeed, we rely upon technology in many ways that are far more mysterious than that in which we rely on technology for authentication. Mr. Guida concluded that, in his view, uncertainty should not be allowed to paralyse action.

Lionel Vodzislawsky, Ministry of Economy, Finance and Industry (MEFI), France[11]

Mr. Vodzislawsky discussed MEFI's work on electronic declarations of value-added tax (VAT) and customs. He first presented the general framework for MEFI's work: He spoke about electronic declarations between businesses and the administration. The project's first goal is to make VAT and customs declarations available over the Internet by the beginning of the year 2000. VAT declarations potentially concern 3 million companies. Each private business has to file a declaration once a month, and small, medium and large companies are all concerned. SMEs, which number between 300 000 and 600 000, are the first target of the electronic declarations project.

Mr. Vodzislawsky then identified several principles underlying the implementation of a PKI. First, any solution must be reliable from a technical and legal point of view and must have an acceptable economic

7. Subsequent to the meeting, it was decided to have GSA perform this task.

8. Due to the change of lead responsibility, this date has slipped to early 2000.

9. Now mid- to late 2000.

10. The first award was made on 10 September 1999 to a consortium led by Digital Signature Trust http://gits-sec.treas.gov current content.

11. For more information, see www.finances.gouv.fr and www.industrie.gouv.fr.

cost for companies. Second is the use of the same signature creation device (*i.e.* the same hardware or software) according to the needs of companies and their own security policies (*i.e.* to set up criteria for the protection of signature creation devices). Finally, Mr. Vodzislawsky discussed the need for certificate criteria.

Elaborating on the first principle, Mr. Vodzislawsky suggested that a single, common ministerial policy for all electronic declarations would make it possible to use the same certificate for several (or all) declarations. Then, in order to address the second and third principles, criteria should be set up to protect signature creation devices. This would involve publication of criteria for certificates and certification service providers and use of a standard external certification policy. The Ministry will set up and maintain a list of compliant certificates, and companies will be obliged to use certificates that comply with these criteria. Outside of MEFI, companies may buy their certificates from any certification service provider that complies with MEFI's criteria (*i.e.* the external certification policy).

Mr. Vodzislawsky noted that the EC Directive on electronic signatures mentions the publication of criteria to protect signature creation devices, and that France, Germany and Italy have been strong proponents of Annex III on electronic signatures. Although electronic submission of VAT declarations does not involve very confidential data, it must be possible to protect companies in order to avoid false declarations and prevent declarations from modification following their submission. Criteria to protect the signature creation device will protect companies. MEFI also wants to use common criteria to determine a protection profile. Further, aware of the need to protect data submitted by clients, MEFI will strongly recommend that companies use compliant products. There is some talk of making this mandatory, but at present, it is only a recommendation.

Within the Ministry, MEFI will set up its own PKI to provide certificates for its employees and servers that deal with electronic declarations. MEFI's PKI will have various entities within and outside the Ministry, including an authority agency, a certification service operator, and an audit and reference entity.

The authority agency is responsible for all PKI use in the ministry. It is a ministerial entity which supervises other entities and the granting of certificates in the ministry. It also supervises the respect of the policy in the ministry.

The certification service operator provides certificates according to the needs of MEFI. The certification service operator will be an external agency, a commercial entity that will work under contract with MEFI.

Finally, the audit and reference entity sets up and maintains a list of certificates that comply with the external certification policy. This entity will also act as an auditor for the certification services operator and will be a commercial entity working under contract with the ministry.

The distinction between the authority agency and the certification service operator is the one made by Warwick Ford at the technology primer when discussing the administrative authority and the certificate utility.

Jacques Pantin, Intervenor

Mr. Pantin discussed market concerns -- the concerns of a businessman -- and raised several questions. First, he noted that 1999 could have been the year of the PKI but is not. There are pilots everywhere but not full deployment. Could 2000 be the year of the PKI? Second, Mr. Pantin noted that, according to market studies, 40-50% of expenses in the security field could concern PKIs by the year 2003. He wondered if he would be rich in 2003 or whether he would have to wait.

Mr. Pantin then turned to the problem of practices. He promotes smart cards because we know how to manage them (*e.g.*,we know how to revoke them). Mr. Pantin suggested that even a very good CPS is not good enough. Next, he addressed risk management. He noted that he faces risks when dealing with another CA in Europe and asked what the appropriate level of "courage" should be. Currently, he trusts the practices of "friends", but as the level of liability is low at present, this is appropriate. However, when the level of liability increases, what will be the appropriate level of "courage"?

Mr. Pantin then spoke about applications. What are the best applications for PKI? What is being done with traditional legacy systems? PKI markets include intranets with 30% of the market, EDI applications (*e.g.*,ANX) with 40% of the market, business-government applications, Internet, ISPs, telecoms, etc.

Robert Fisher, Intervenor

Robert Fisher began with a quick overview of PricewaterhouseCoopers' activities. It recently completed a study on the business environment for electronic services, which focused on the role of government and the obstacles to electronic services from a market perspective.[12] It is currently engaged in a large project in which it acts as a CA for the EU and issues digital certificates to SMEs, students, businesses, etc.[13] It is paying particular attention to the market aspects of its activities, focusing on why people do or do not want to use these services.

Mr. Fisher raised three questions. First, he asked, "What are you doing to raise user awareness?" He remarked that we hear about technology, interoperability and other technical topics but not much about users. Consumers need to know what a certificate is, what they can do with a certificate, and what their risks, costs and benefits are. Mr. Fisher noted that, in most situations, getting a certificate is voluntary.

Mr. Fisher's second question focused on appropriate use of PKIs. He asked the panellists whether PKI should replace all authentication or only authentication for high-value transactions (*e.g.*,where privacy of medical records is involved). Mr. Fisher noted that although it seems that PKI and digital certificates are needed for everything, he thought that these technologies are not needed for many low-value transactions.

Finally, Mr. Fisher asked the government representatives on the panel to elaborate on the factors they take into account when making decisions about whether to outsource PKIs and parts of PKI services.

Responses

Mr. Richard Guida responded to Mr. Fisher's second and third questions. In response to the second, he stated that the concept of technology neutrality applies, *i.e.* the technology that is suitable to the transaction should be used. In some cases, a PKI is not needed, and in others, it might be desirable. In particular, Mr. Guida noted that a PKI may be desirable when there is a need to scale because shared secrets such as PINs and passwords are not easily scaled. In addition, to the extent that users want universal use of strong authentication, PKI is a good solution. Thus, a PKI meets DoD's needs. PKI also is good for infrastructure protection; where critical infrastructure must be protected, a PKI may be needed.

Mr. Guida then addressed the third question, noting that, in the United States, law enforcement tends to want to operate in-house while agencies tend to like outsourcing. It was decided that the National

12. For more information, see http://www.bests.org .

13. For more information, see www.fp5-csp.org

Telecommunications and Information Agency (NTIA) will run the PKI because some agencies may not interoperate through a bridge run by a private sector entity.

Mr. Tiga Tita then answered Mr. Fisher's question about user awareness. He explained that G77 uses the chamber framework (hierarchy of trust among members) to address user awareness. G77 relies on the chamber framework in order to reach consumers. As an example of how this works, he noted that there are 1 500 chambers in Brazil, each of which will have a city workshop with its own members. User awareness might be improved at a city workshop, or at another, more local, level down the hierarchy. Thus, user awareness can be addressed through the chamber hierarchy. The Chamber Network expects to have issued 800 000 to 1 million certificates before next year and hopes that there will be a community of users using chambers as a reference.

Peter Stokes, Intervenor

Peter Stokes offered an SME perspective. He began by recalling that Hong Kong, China, is the fifth largest trading economy in world, so that facilitation of trade is very important to it. He remarked that there had been little reference in the presentations to how electronic authentication would facilitate trade.

Mr. Stokes then emphasised the importance of SMEs in Hong Kong, China, noting that of its 70 000 importers and exporters, 98% have fewer than 50 employees and 87% have fewer than ten.

Mr. Stokes explained that Tradelink processes trade documents in a secure way. Tradelink's customers are importers and exporters, and a key need is a message delivery system. Currently, before Tradelink can issue public-private keys, it must receive various paper documents, including a business registration certificate. If these documents were electronic, other certificates could be done electronically. Thus, Mr. Stokes emphasised the need for acceptance of standard international trade documents (by importers and exporters) in electronic form without their paper counterparts.

In continuing, Mr. Stokes pointed out the need for authenticated identities and noted that much work has been done on PKI development. He stressed that a PKI must be in place before applications are rolled out (*i.e.* he supports Canada's top-down approach). However, he asserted that these infrastructures are incomplete until all government-issued identity documents are acceptable in electronic form.

Responses

Mr. Richard Guida responded as follows. First, he noted that, in the United States, there is a "strong loathing" of the idea of a national identification card. ACES (discussed above) carefully avoided the appearance of being a national identification card. Indeed, ACES certificates do not include a person's name or social security number, but only a common name.

Mr. Guida then offered a reaction to the suggestion that the authentication element be harmonised. He said that the United States does not see a harmonisation of the authentication element. He explained that the premise in the United States is that the credential is not unique. Although multiple credentials will have less utility than a unique one, Mr. Guida asserted that the United States will continue to have multiple credentials.

Mr. Kakulavarapu of ANX responded that many standards are being developed, and none is unique. For EDI alone, there are 180 standards. If a global ID number is desired in order to interoperate, a standard will be needed. Otherwise, each company will create a number of different lengths, thereby raising barriers to interoperability. Thus, there may be a need for a standard ID around the globe.

Mr. Tiga Tita of the G77 Chamber Network also responded. He reiterated that his presentation dealt with the seal and who issues the seal. He said that PKI needs an institutional framework, a trust hierarchy. A central authority and a chain of trust that flows everywhere are necessary. This is why it was thought that the UN might be the place for a global root, with different countries serving as CAs and institutions creating a chain of trust. In Geneva, there was no agreement about whose technology would be used for a global root. While this debate was going on and no-one would accept a global root at the UN level, G77 took a decision and now has a G77 root based in Australia. G77 will use that root with the chambers of commerce serving as a chain-of-trust hierarchy.

Mr. Weigelt of Canada noted that PKI technology is fairly complex, and it might be easier to educate users if PKI disappears and is simply a part of secure electronic commerce delivery. Mr. Weigelt also suggested that it is important to look at PKI in an applications context. In his view, PKI is not the whole solution, as it addresses some problems, but not all. For example, Mr. Weigelt suggested that the import-export issue may be an application issue.

Finally, with respect to the outsourcing issue, Mr. Weigelt said that in making this decision, Canada is concerned about liability. The government starts out with a costing model and looks at assurance levels. When the government deals with industry and the populace, concerns include ease of access (*e.g.*,Is registration easy?), trust (*e.g.*,Will people trust the police service to register people?[14]); freedom of choice (*i.e.* the Canadian government would like to allow people to choose how they interact with the government).

Mr. Kakulavarapu added the need for high security, support, agreements and contracts, and said that companies outsource so that they can concentrate on their own businesses.

Mr. Ferguson asked each of the panellists to identify a priority to be added to the OECD work plan.

Responses

Mr. Tiga Tita wished to see the OECD come to the table to talk about a global root certificate.

Mr. Kakulavarapu's priority was to figure out how to advance the legal processes that enable global business. ANX is looking at a global economy and an open market, and service providers, product suppliers and users need to be protected. He recognised the difficulty but emphasised the need to work towards this goal.

Mr. Guida applauded the efforts made in the workshop and suggested that the OECD sponsor additional opportunities to share experience and activities. He stressed that such meetings should not simply be educational but allow participants (especially those seeking to deploy PKI) to sit down and study various approaches.

Mr. Weigelt of Canada's PKI Task Force felt that there is undue concern about liability. People are afraid to move forward because of this, and he suggested that the OECD could take a role in mitigating this fear.

14. This is the Finnish approach.

Session V: Global Policy Issues

Moderator

- Stewart Baker, Steptoe & Johnson, LLP

1. SUMMARIES OF SESSIONS I-IV

Mr. Baker asked the moderators from Sessions I-IV to summarise the main points that emerged during these sessions.

Session I

Session I provided an update on recent developments in the area of electronic authentication. Ms. Teresa Peters reminded the audience that Session I included a discussion of trends in private-sector initiatives (Mr. Yoshikawa, GBDe), APEC activities (Mr. Orlowski, Electronic Authentication Task Group, APEC), EU activity (Mr. Schlechter, DG XIII, European Commission), UNCITRAL (Ms. Clift), national legislation (Mr. Kuner, Morrison & Foerster LLP), and private sector standards initiatives (Dr. Fumy, Chairman, ISO SC27).

Ms. Peters noted that Session I looked at legislative, technology and policy trends. In the legislative area, Mr. Kuner noted the shift from prescriptive (detailed, technology-specific) laws towards technology-neutral laws. In the technology area, discussion emphasised the use of authentication methods appropriate to the transaction (*i.e.* varying the levels of security based on the requirements of the transaction) as well as a trend toward hybrid authentication (*e.g.*,combinations of biometric and smart card authentication). In the policy area, Ms. Peters identified the tension between the need for uniformity and harmonisation (driving standards activity), on the one hand, and the desire for flexibility (driving competition), on the other. She then noted the trends towards interoperability which attempts to accommodate both uniformity and flexibility. Two potential roles for government were mentioned: government procurement could help drive electronic commerce and government could provide a forum for standards development activities. Finally, Ms. Peters noted that participants emphasised the importance of both non-discrimination and consumer issues.

Session II

Session II focused on case studies in the financial services sector and other service industries. Mr. Brian Smith first observed that his summary was necessarily influenced by his perspective which, in turn, was shaped by his professional experience, including his work for Visa and later as General Counsel at Mastercard. Indeed, he was involved with the electronic delivery of financial services when the law only governed consumer protection, and not relationships.

Mr. Smith identified several trends and conclusions that emerged from the presentations in Session II. First, financial institutions have a trust relationship with their user base. Second, there are two different models for the role of financial institutions in electronic authentication. One is the hierarchical, or co-operative, model exemplified by Identrus which is driven by allocation of risk, liability considerations and the allocation of responsibility. This model focuses on business-to-business transactions. The second model is the direct delivery of services, a model in which an institution deals directly with consumers.

Banks using this model, such as ScotiaBank and NordBanken, deliver services directly to their customer base. This model is concerned largely with ease of use and focuses on business-to-consumer transactions.

Six policy issues were raised. First, there is a need for basic principles to provide certainty about the effect of electronic transactions. The principles need not necessarily be intrusive, but they should establish a minimal level of expectations as to what an electronic signature means. Second, there is the importance of risk allocation and management. This does not mean that there is a need for a new regulatory structure as some is already in place. Third, there are the related concepts of international co-operation and non-discrimination. Emphasising that each panellist talked about a different way to do business, Mr. Smith indicated the need for common acceptance of different approaches and diversity, *i.e.* non-discrimination. Fourth, in Europe, notaries serve an important function, and notary associations have already developed a system to deal with that very personal service. Fifth, two separate possible roles for government emerged from the panel. In the first, government acts as incubator (what Ms. Peters referred to as government as facilitator). In the second, more passive role, government simply keeps an eye out for problems. Sixth, and finally, Mr. Smith noted that the participants in Session II identified consumer protection, privacy, and homogeneity across borders as very important issues.

Session III

Session III focused on authentication in organisation-to-individual transactions. Mr. Claude Boulle first stated that the main challenges to authentication between commercial entities and the public are cost and consumer acceptance. He reminded the audience of Mr. Rubenstein's discussion of online shopping as an example of an area in which authentication is not yet ready to emerge, an area where there is not yet a need for customer authentication. While several presentations were about local initiatives, speakers recognised the potential for cross-border activities. There are major joint initiatives between the government and the private sector to develop and share authentication infrastructure on which different applications will be built for different communities of interest. Within the shared infrastructure (*i.e.* shared PKI), policy differentiates applications and is defined by the operators delivering the services. Finland, Norway and Sweden are implementing this type of shared infrastructure, but for three different applications, one of which is government online. This shared infrastructure approach demonstrates the scalability and versatility of the architecture that has been endorsed by those three countries. Finally, Mr. Boulle noted that there was unanimity about the need for more standards.

Session IV

Session IV focused on organisation-to-organisation (business-to-business and government) transactions. Mr. Peter Ferguson identified several major themes. The first is that authentication should be seen as a policy issue and not just as a technology issue. The discussion during Session IV strongly indicated the need for more discussion of how electronic authentication will facilitate business (business development vs. policy) and the importance of increasing awareness of authentication not only as a technology exercise, but as a policy issue.

The second is the issue of whether governments should take a top-down or bottom-up approach to rolling out electronic authentication. The top-down approach is exemplified by Canada's "build it and they will come" idea while the bottom-up, pragmatic approach is evident in the US decision to let agencies choose among various models.

The third involved business-to-business transactions. There is a need for global business models and basic, internationally accepted agreements, principles and, in some cases, rules to facilitate electronic commerce. Conversely, it is necessary to minimise the impact of national and local policy on international activity.

The fourth major theme focused on the need to build trust and confidence. Mr. Ferguson noted that panellists repeatedly emphasised that there is more at stake than security; the issue is building trust and confidence in the marketplace. Mr. Ferguson suggested that confidence can be built by providing adequate information so that parties will learn to trust each other. Further, for the ease of users, some commonality would be useful.

Other themes that emerged from Session IV included the idea that authentication must be useful throughout one's lifetime (*e.g.*,via archival and backward compatibility), that authentication should trust no-one and that liability issues must be addressed.

Mr. Ferguson concluded with three observations. First, there is a continuing need for norms, guidelines, and principles to facilitate the development of global business. Second, confidence and trust building needs to continue both in the policy arena and in terms of awareness-raising. Third, although this may represent a shift in the OECD's role, the Organisation should sponsor and engage in more information-sharing activities such as this one, creating opportunities for information sharing involving other international bodies.

2. GLOBAL AUTHENTICATION IN THE CONTEXT OF THE OECD OTTAWA MINISTERIAL DECLARATION

Moderator

- Mr. Stewart Baker

Presenters

- Mr. Norman Reaburn, Workshop Co-chair; Chairman, OECD ICCP Committee's Working Party on Information Security and Privacy; Deputy Secretary, Attorney General's Department, Australia
- Mr. Ed Zeitler, Workshop Co-chair and Senior Vice President, Information Security Services, Charles Schwab

Panellists

- Andy Pincus, General Counsel, Department of Commerce, United States
- Masanobu Kato, Fujitsu; Chair, Internet Law and Policy Forum (ILPF)
- Hubertus Soquat, Ministry of Economics and Technology, Germany
- Supriya Singh, Senior Research Fellow, Centre for International Research on Communication and Information Technologies (CIRCIT), Australia
- Fuminori Inagaki, MITI, Japan
- Laurent Jacques, French Ministry of Justice
- Joe Alhadeff, previously involved in USCIB e-commerce issues, now Senior Director, Global Public Policy, Oracle Corporation

Norman Reaburn, Co-chair

Mr. Reaburn, the Workshop Co-chair and Chairman of WPISP, began by noting that, like Mr. Smith, he has mediated through his own experience the topics discussed during the workshop. Mr. Reaburn mentioned two aspects of his background that are of special significance. First, he is a bureaucrat, and second, he is a lawyer. Also, as a long-time academic, he has some experience with certain aspects of the elements of the systems being discussed.

Mr. Reaburn first noted some inherent tensions. Anyone using the Internet for business or government purposes needs trust and certainty, yet the nature of the Internet is such that these are either regarded as not important or they are diffused. Next, he described a shift in the purposes for which the Internet is used. It was originally devised as a means of routing messages through devastation. In that context, people did not worry about systems or certificates although the messages they planned to send were as important, if not more important, than the messages that have been talked about. The Internet later moved through a period marked by a combination of research and anarchy, the period to which Ms. Radin referred in her keynote address. Today, there is a third layer, the use of the system for electronic commerce. A system that began as a means of dealing with chaos has become a means of developing electronic commerce.

Electronic commerce, according to Mr. Reaburn, is based on a combination of technology and an information economy, a new basis for government and private activity. What is new about the information economy is the digitisation of information and a new mode that ensures speed and volume. We are witnessing the transformation engendered by the extraordinarily powerful combination of a significant technology and a significant mode.

Mr. Reaburn discussed five important consequences of electronic commerce. First, electronic commerce encourages certainty; it encourages certainty in the regulatory framework, harmonisation and convergence. As global activity increases, reactions to activity are likely to be similar throughout the world, so that there is a strong push towards harmonisation and convergence. Mr. Reaburn noted that the business component of that push has been tied up with cultural components. Although the two components could be kept distinct, they are not being kept distinct, and policy makers need to keep this in mind.

The second consequence of electronic commerce, said Mr. Reaburn, is that there is a sense that anything that can be turned into information should be. Indeed, one of most significant developments in financial services in the last few decades is that money is now information; physical money may gradually go out of style. Similarly, music is now information. Indeed, a whole range of things can be turned into information and therefore traded in a new way. As a result, there is potential to strip product mystique out of these things and to replace it with technology mystique.

The third consequence of electronic commerce that Mr. Reaburn mentioned is the speed component, which has made paper-based processes a chore. Personally, he uses the telephone or e-mail, as he finds writing a letter a chore. When and if a task cannot be accomplished via e-mail or with a telephone call, there is a real chance that it will not get done. Similarly, complaints in writing to agencies are far less numerous than telephone complaints.

The fourth consequence of electronic commerce is the disappearance of boundaries. The “On the Internet, nobody knows you’re a dog” cartoon mentioned by Mr. Tiga Tita indicates that a boundary has disappeared. Geographic boundaries also have disappeared, and relationships no longer need to depend on geography, but can depend on interests. Indeed, all kinds of groups around the world come together on the basis of interests.

Finally, electronic commerce leads to non-hierarchical organisation. Indeed, if electronic commerce is an information process, one never knows what the source of the next good idea will be, and one has to be able to get it.

Mr. Reaburn next turned to a discussion of the impact of law on levels of authentication. He noted that, except Mr. Fitzpatrick, by implication, no-one talked about law enforcement (including issues such as fraud and computer crime) or lawyers. Lawyers are concerned that any particular piece of a transaction might end up in the legal process (*e.g.*,be challenged in a court). As a result, there is pressure to increase levels of authentication. This tendency to push authentication levels upwards is to be contrasted with the point forcefully made by a number of speakers that technology should be used appropriately for the transaction and that the parties involved are the best judges of that. Mr. Orlowski gave an example of the latter proposition when he described a circumstance under which a party viewed e-mail as appropriate authentication; the party was prepared to act financially -- to come to a USD 2 000 conference -- on the basis of an e-mail invitation.

Mr. Reaburn next turned to issues of privacy and anonymity. He noted that in the old "village", a person's activities were limited because everything people did was known within the community. In that context, one could not hide who one was or what one did. However, we have been moving away from that model for some centuries and enjoying privacy and some anonymity in certain aspects of life. Technology has the potential to return us to the old village in that everything we do can be logged and checked. For example, Mr. Guida spoke about 2 million people with certificates in the Department of Defense. Thus, everything they do can be structured so that their activities can be checked. Mr. Reaburn suggested that privacy and anonymity should be context-dependent. For example, the DoD does sensitive work and should be able to ensure that there is no interference with that work at any time. In other contexts, more privacy may be appropriate. In the law enforcement context, fraud certainly would be reduced if everything were watched, but a balance is needed. However, technology is making the balancing exercise more difficult.

Mr. Reaburn then suggested the utility of considering whom the government is addressing when it takes a policy position. The whole community? The legal system? People do not worry about whether there is a back door on the bank vault, but they worry about a back door on an electronic vault. That is what he meant by replacing product mystique with technology mystique.

Finally, as Jeremy Hilton noted in Session III, the debate must be about business benefits, not technology. We must be clear about our objectives. Once we are clear about our objectives, the technology locks in.

Ed Zeitler, Co-chair

Mr. Ed Zeitler began by saying that he was addressing the PKI community, of which he is a member. He said, "PKI is the solution; now what is the problem?" This workshop was designed to address not the question of how to build a PKI correctly but larger issues. It is necessary to take a global view in order to make any progress; countries that do not participate in electronic commerce will not keep up economically.

Mr. Zeitler noted that two communities are investing in solutions: government agencies and business. For the successful deployment of large PKI systems, one needs discipline, reason and logic and he suggested that these come from government agencies not from business. Government tends to identify and solve all possible problems before deployment, whereas business tends to solve only the problems they encounter. Concentrating on this difference between government and business, Mr. Zeitler asserted that two approaches are needed to the PKI and electronic authentication mechanisms. Government plays a key role in international business. Its ability to facilitate the flow of goods and funds using electronic means can significantly affect a country's economy. Further, issuance of a certificate requires discipline, reason and

logic. However, assigned credentials must be able to be accepted (*e.g.*,a business license may need worldwide recognition). Governments agreed on the form of passports but probably did not agree on the criteria or the process for obtaining a passport in any country.

Mr. Zeitler suggested that OECD has a major role to play and that it will address these issues effectively if it understands its role.

From the business perspective, Mr. Zeitler asked, "What are we authenticating?" He noted that there are significant differences between authenticating people, corporations, businesses, systems or machines. Many different solutions are available to address this issue. However, for those who are thinking about business at present, the problem is authenticating individuals. Public key cryptography appears to be a good choice, but delivery, control and manufacture of public keys are not yet viable. In addition, the current approach to public key cryptography has made TTPs necessary. However, Mr. Zeitler suggested that a new standard might use public keys but do away with TTPs. He noted that at present, the software where the key resides is authenticated, rather than the machine or person carrying out the transaction. To resolve this problem, certificates were put on tokens so that they were not tied to the software using the certificate. As a result, we now have floppy disks and high security smart cards, but these simply authenticate the fact that the person on other end of the transaction possesses the device (*i.e.* the disk or smart card). In order to solve that problem, password protection was added, so that the device would not be activated without the correct password. In view of all of this, Mr. Zeitler asked, "Why not just use a password?" Simply relying on a password is a business solution. This would facilitate non-repudiation without a PKI. His point was that the private sector desperately needs time to develop electronic commerce models and processes. The private sector does not need regulations and standards for PKI. Interoperability of PKI is at the top of the list, but it is interoperability that weighs the private sector down.

In closing, Mr. Zeitler said that the OECD has made a tremendous effort to pave the way for economic growth among nations using the PKI solution that seems appropriate. However, he asked the OECD to refrain from providing guidelines to the private sector this year. The private sector, he said, is not ready for them.

Mr. Masanobu Katoh described ILPF as an international non-profit organisation established by companies interested in promoting electronic commerce. ILPF is composed mostly of in-house lawyers from major international companies; it is not an advocacy group. It tries to examine issues for substantive ideas so that it can develop policy solutions. ILPF has published many papers, including a survey on regulation. Mr. Katoh then explained what has been done at ILPF in the authentication context. Most recently, experts from international business, government, intergovernmental organisations and universities developed consensus principles for authentication. These principles include: *i)* removal of legal barriers to electronic authentication; *ii)* respect of freedom of contract and parties' ability to set provisions by agreement; *iii)* harmonisation to make laws governing electronic authentication consistent across jurisdictions; *iv)* avoidance of discrimination and erection of non-tariff barriers; *v)* allowing for use of current or future means of electronic authentication; and *vi)* promotion of market-driven standards.

Mr. Baker asked, "Where should we go from these principles?" In response, Mr. Katoh said that during the workshop, it has been noted that authentication technologies are evolving, although some are used widely. Mention has been made of policy and technical challenges in specific applications. In Japan, for example, there is a long tradition of using *hanko* (stamps) for certain types of official documents (mostly for government purposes). Mr. Katoh expressed the view that it is necessary to study different systems and identify the potential impact of electronic authentication on legal systems and society. In his view, not all countries are at the appropriate stage to implement globally compatible authentication technologies.

Mr. Baker then turned to Mr. Joe Alhadeff who was involved in the Alliance for Global Business (AGB) principles and the ILPF principles. Mr. Alhadeff explained that the AGB principles demonstrate a broad consensus by business and are in harmony with the principles of the OECD's Ottawa Ministerial. However, the AGB principles are very broad, and disagreements arise when dividing up responsibility for regulating.

Mr. Alhadeff encouraged a shift in focus from "harmonisation" to "harmony". Harmonisation could mean moving to a "low common denominator", or it could mean using a "high common denominator." However, Mr. Alhadeff suggested that there is already harmony of principles in that there is a general understanding at the level of principles, but not at the level of details. He indicated that it would be useful to flesh out the details before doing more. The market needed more time to "shake out".

Mr. Baker turned next to Mr. Hubertus Soquat, who confirmed that Germany is not going to take legal action to restrict the use of strong cryptographic software. No legal restrictions are in place in Germany (*i.e.* cryptography is already free there), but there has been national/international discussion regarding encryption restrictions and the issue has been hotly disputed. Mr. Soquat suggested that the United Kingdom, France and the United States apply pressure to their governments.

Mr. Baker reminded participants that there will be a report from the security services in two years and asked, "Is this just a fig leaf or could it be the basis for change?" Mr. Soquat responded that the German government would return to the encryption issue if necessary. Mr. Baker then asked whether there is a plan to test products differently from what is currently done. Mr. Soquat responded that he was defending a difficult, developed legal and technical system with infrastructure behind it.

Mr. Soquat added that many people spoke about trust, confidence, security, verification and verified security, and, taking it all together regardless of some differences, he felt confident. He did not think that different models divide the world in two. He felt that there is some convergence and solutions that give government, business and users confidence. The OECD should look at transparency and look to the future. Market forces should be allowed to operate and there should be competition among concepts. Nevertheless, Mr. Soquat argued that a framework is needed for the new technology and that is what governments are for. He also told the audience not to forget access issues which affect both the G77 countries, who are in a different situation economically speaking, and the disabled.

Mr. Baker then asked the panellists to address the government's future role in electronic authentication. During the workshop, possible roles suggested for government included building trust, sharing information and creating certainty. If government adopts one of these roles, how should it accomplish its task? Via standards? Should it stand back and create a greenhouse for new models of authentication? Should there be an elaborate set of government agreements on what is acceptable authentication?

Responses

Mr. Andy Pincus began by adding to Mr. Reaburn's earlier statement about the characteristics of the Internet. In addition to being speedier and handling higher volume than other technologies, it is empowering as well; it allows complete freedom for very different business uses. This freedom is a critical aspect in any discussion of the government's role. The government's role is to enable the various business uses, most obviously by establishing standards for the legal enforceability of contracts. When people engage in contracts, they want to know that the contracts will be legally enforceable. To ensure legal enforceability, the government simply needs to eliminate the requirements for pen and ink signatures. That is as far as governments should go. There are many different models for authentication, and it is quite difficult to choose a model or a technology. Even if a PKI is chosen, there are hundreds of steps in the PKI

system that may require different approaches. Thus, on the legal front, the government should stand back so that people can choose authentication models appropriate for their transactions.

Mr. Pincus then distinguished between the government as a market participant and the government as a regulator. When the government is acting as a market participant, it may choose the appropriate authentication (*e.g.*,it chooses authentication for the government to use to provide government services). Finally, Mr. Pincus noted that with respect to legal standards for when a contract is legally enforceable, there is no magic bullet in the electronic or the physical world. However, Mr. Pincus emphasised that we want bridges so that there are clear pathways that allow contracting internationally.

Mr. Baker asked Mr. Jacques what is required in France to allow use of electronic authentication. In particular, how would the French system accommodate or interact with the minimalist system that Mr. Pincus is describing? Mr. Jacques replied that the French approach is somewhat different from those discussed during the session. French people think that government can intervene without limiting the technological revolution. Mr. Jacques asserted that governments need to intervene to provide legal certainty. The French wish to avoid a situation in which an electronic signature will be challenged every time it is used. In addition, judges often will not have expertise in the field of electronic signatures and will have to call on outside experts. According to Mr. Jacques, it is therefore more useful to deal with the problem "upstream".

Mr. Jacques suggested that among the range of legislation presented at beginning of the workshop, France takes a middle position, *i.e.* recognition of legal effect in the framework of the EC Directive on electronic signatures. According to Mr. Jacques, France agrees with the framework for non-discrimination (*i.e.* it recognises a digital signature regardless of the device used) but there should also be a higher level of recognition for technologies that meet higher criteria. France is trying to adapt its Civil Code in light of this. There has already been work to allow for the use of electronic signatures. France has various rules that prevent the use of electronic signatures for transactions beyond USD 900 (not a high threshold) and between businesses and individuals. Currently, everything has to be on paper, but France is trying to modify the notion of what it means to have a written signature so that it will be possible to consider an electronic signature as equal to a written one. Having said that, Mr. Jacques stipulated that this will not be placed in the Civil Code, in order to maintain technological neutrality. Technology is evolving quickly, but bureaucrats adapt slowly. However, the French want to include some provisions concerning electronic signatures in the Code. France will comply with the EC Directive, which will force all member states to adopt a similar policy in this field.

Mr. Baker then asked the panellists to suppose that a company stated, "We use passwords to authenticate customers. We do not need an elaborate PKI system to identify customers and take their orders." To begin the discussion, Mr. Baker asked if that would be possible in France, or if the company would be required to take orders using the kind of system discussed earlier.

Mr. Jacques replied that electronic commerce is developing in France slowly but surely. The problem in France is a problem of the rules of evidence. Where there are agreements among parties, there is no problem. That is, when prior agreements have been made, there is no problem because the rules of evidence are flexible and it is possible to allow for closed systems. However, in business-to-consumer relationships, there could be a problem because the Civil Code currently requires a paper trail, and this tends to slow the use of electronic transactions. In France, it is difficult to provide sufficient proof that Civil Code requirements have been met. This will change, so that those who fulfil certain criteria will be able to enjoy certain benefits. If you use certain authentication techniques, you will get benefits.

Mr. Inagaki explained that in Japan, MITI, MPT and MOJ will co-operate to establish a framework in which electronic signatures have the same legal effect as handwritten signatures or a seal/stamp. Indeed,

Japan is contemplating extending the reach of the existing Japanese legal framework for contracts so that it covers the virtual world.

Under Japan's current framework, when a seal is affixed to a document, there is a legal presumption that the document is genuine (*i.e.* a stamp has a kind of non-repudiation effect). The stamp system provides predictability. Once a stamp is affixed to a contractual document, there is no need to worry about the conclusion of the court in the event of a dispute. Japan believes that the same legal effect (*i.e.* a legal effect analogous to the presumption for documents with seals) should be granted in the electronic world. Mr. Inagaki also noted that there are no form requirements in Japan. Any mutually agreeable means for concluding a transaction is sufficient. Only mutual intention is required. This parallels the common law for most contracts. Mr. Inagaki agreed with many speakers that authentication is a policy/business issue rather than a technology issue.

Ms. Supriya Singh spoke from a consumer perspective and noted that the concept of trust is a useful bridge. She pointed out that authentication – knowing with whom you are dealing – is a minimum condition of communication. However, she suggested that it may be necessary to broaden our discussion if we are truly embarking on a new way of living, communicating and working.

Consider the user's perspective. People do not say that they will not make purchases online because transactions are "not authenticated", in part because of users' perspective. People are interested in what the new technology means for activities, relationships, health, education, etc. They will use whichever channel suits them best. For example, people will not purchase some things without a receipt, but they will purchase other things in cash without a receipt. This is (in the payments context) the "web of trust". Businesses are worried about authenticating the consumer, but the consumer wants businesses to be authenticated. The consumer wants to know that the business is legitimate or that it received a payment. Ms. Singh argued that if authentication technology works, businesses should say this to consumers and take the risk of guaranteeing it. Businesses have not yet done this.

Markets may work these problems out, but, as Ms. Singh remarked, markets are social institutions. An understanding of the social aspects of authentication is needed, particularly with respect to factors that allow people to trust. We need an understanding of trust because people want to authenticate what they do not trust. Originally, people said that credit cards – "plastic money" – were not real and they were not trusted. Today, people interviewed about money say that credit cards are real, or trusted, but they do not trust sending card numbers over the Internet. Banks have had electronic money for decades and people did not talk about authentication. Now that electronic money is in the home, authentication has become an issue.

An Australian study, *Gender, Design and Internet Commerce*, found that a trusted technology changes the nature of an activity. When people were asked how they communicate, they described how they communicate over the telephone. However, for many of the world's countries, communication over the telephone is not real.

Referring to Mr Reaburn's point about the disappearance of boundaries, Ms. Singh added that the global nature of electronic commerce does not necessarily mean the disappearance of boundaries. Indeed, it may mean the appearance of new boundaries based on cultural differences and the level of trust people have in different kinds of electronic communication.

Mr. Baker then proposed a tentative point of consensus. He suggested that there might be consensus regarding the importance of different levels of trust for different levels of technology. He noted that this would be consistent with the minimalist approach outlined by Mr. Pincus of the United States, the two-level approach described by Mr. Jacques of France, the ILPF's approach of honouring contracts and giving

basic effect to electronic authentication, and the approach, which the Japanese government may take, of granting a presumption to certain technologies, but recognising signatures of all sorts.

Mr. Alhadeff responded to the suggestion of "tentative consensus" by noting that, given the composition of the workshop, there might be apparent consensus. However, there might not be consensus if the workshop had a participant from a business's marketing department. Mr. Alhadeff commented that in the real world, companies are very reactive to customer satisfaction.

With respect to trust, Mr. Alhadeff noted that the concept of money has been based on trust ever since gold was used. Business and government may now take new roles in building trust, and business agrees that that is a role that government plays. Having noted that efforts should be industry-led and market-driven, Mr. Alhadeff identified a twofold role for government. First, at certain times, government action is as important as government forbearance. It depends on what is important at what time. Second, government action should seek to facilitate; it can level the playing field, creating some levels of equivalence. Or, it can provide some basic certainty. Mr. Alhadeff recommended that "level playing field" problems should be addressed before addressing questions of legal presumption.

Mr. Baker then asked if anyone disagreed that a way is needed to ensure that if one signs with a password, the signature receives basic recognition in every country. Mr. Soquat replied that electronic communication is not a completely new world. In the paper world, there are also problems between different legal systems. Thus, ways should be sought to bring things together without harmonising every single national law.

Mr. Pincus stated that for a volume of cross-border transactions greater than the world has yet seen, the body of law should be as user-friendly as possible, and there should be some certainty, or some way to achieve a reasonable level of security. He felt that contract-based systems might attain this goal. If people agree to be bound by some method of authentication in subsequent agreements, then subsequent contracts will be legally enforceable. Indeed, contract-based systems may be the critical bridge.

In addition, Mr. Pincus noted that even if countries adopt presumptions, they must make sure that those presumptions do not disable the use of other technologies. For example, if he were to use a password to enter into a contract with Charles Schwab, he should have the opportunity to prove that he entered into the contract and that he intended to be bound. He proposed that one would be subject to a higher burden of proof if one used less technology. If a company built a more secure system (*i.e.* a better mousetrap) that was not entitled to a presumption, it still could rely on that system if it was confident of proving its validity.

Mr. Baker asked whether that would be enough to satisfy legal certainty.

Another participant asserted that everyone is afraid to say there should be any regulation because it may be best for the market first to sort itself out. He suggested this is a "meagre" result from a workshop. His concern was the role of the trusted third party, not so much as a giver of certificates, but as one who takes responsibility for trust in transactions with other countries. His concern was the regulation of the trans-border experience.

In reply, Mr. Alhadeff said that while it may be a "meagre" resolution, that is where we are. The minimalist approach cuts across all of the models and therefore is an appropriate place to start. A shakeout and more information are needed. In terms of regulation of the trans-border experience, Mr. Alhadeff's position was that regulation may be a barrier. However, Mr. Soquat recalled that the technology is already available and indeed, the availability of the technology was the principle underlying the German system. Germany takes verified components, etc., and on that basis, awards legal recognition. Germany builds trust

on this basis. The approach is advantageous because there is a common market and Germany needs a solution that will work globally.

Mr. Baker then took another "cut" at consensus, suggesting that in the business-to-business context, there is broad agreement that if two businesses enter into an agreement about authentication, no country would modify that agreement. Given that, there is not much role for governments to set standards for business. In the business-to-consumer context, there is concern that requirements will interfere with a global system that works across borders. Is there agreement on what governments should be doing with their citizens?

Mr. Katoh noted that there are many national, regional and legal challenges. In many areas, the business-consumer relationship is based on practice or customs and it may be useful to take a fresh view. For example, some areas really require *hanko*, but in many, stamps are simply used because they instil confidence, although they are not legally binding. Mr. Katoh added that the role of government is to build awareness through education and to build confidence.

Mr. Pincus then addressed Mr. Baker's comment on business-to-consumer transactions. He noted that in the credit card model, consumers can be bound for more than USD 900 as long as that is fair. He saw no reason why the principle could not work for electronic transactions as well. In his view, the government's role is to focus on transactions between government and citizens, and with respect to those transactions, the government should pick the kind and level of authentication that is appropriate to that context.

Mr. Jacques noted that the workshop dealt with very technical questions. It also focused more on the variety of experience than on legal issues. Therefore, it was difficult to draw conclusions on legal aspects of authentication, as they were only addressed tangentially. However, these legal aspects are addressed by UNCITRAL, and some efforts to reach harmonisation are under way.

Mr. Jacques expressed his view that the government should facilitate electronic authentication. However, he does not think that government's role is limited to facilitating authentication through procurement policies but that it also has a role in protecting consumers.

Mr. Kakulavarapu noted that if he has to deal with different PKIs, different concepts and different rules, it is too difficult to do business. If he has to understand how the PKI is implemented in different countries, it is too much of an obstacle. Mr. Baker asked whether the problem would be solved if the rule was, "If you have an agreement, we'll enforce it."

Mr. Field noted that everyone nodded when Mr. Baker asked, "Don't we agree that for business-to-business transactions, there should be no need for regulation if they both agree?" Yet, in the one model that was developed with substantive input from banks and corporations, that was not developed.

Ruth Day, Executive Director of ILPF, said that she suspects there is a reason to think there might be a discrepancy in bargaining power at the time a rule is made. She suggested that discrepancies be allowed to appear and that there should be a presumption of non-interference unless there is a strong reason to interfere.

John Dryden asked, "When do we want to do a non business-to-business transaction across Member countries?" Mr. Baker responded that this would happen if an individual wanted to sell USD 900 worth of goods to a Frenchman over the Internet. He suggested that countries that decide to give preferential treatment to certain types of signatures may put themselves at a disadvantage.

Mr. Alhadeff pointed out that it is sometimes assumed that because criteria have been adopted, they are neutral. He stressed that if the criteria chosen are very narrow or specific, this may not be so. He argued that countries may create obstacles to trans-border deals if they do not address a broad range of

transactions but only a narrow subset. Thus, in dealing with a specific problem, a country may have developed a facially neutral regulation that has discriminatory effect in application.

Mr. Soquat responded that this is not a simple question of discrimination. Rather, it is a question of predictability and certainty. If you have to go to court, the German system offers the advantage that you do not need to prove the validity of the signature in court using experts. The judge will simply allow the signature to stand. He suggested that the World Trade Organization is the proper forum to discuss obstacles to trade. Mr. Baker quipped that this may be the first industry in which there may be a trade war before anyone has made a profit.

Mr. Pincus then asked, "If two companies agree, why not enforce the agreement?" It would be a tremendous obstacle if, to do business in Germany, companies have to meet requirements that it is physically impossible for them to meet.

Mr. Schlechter clarified that if Germany has a mandatory law, the German law must be followed, because under the Directive, one has to fulfil the written form requirement. But, in all other areas (*i.e.* except the written form requirement), this would not be the case. That is, in all other fields, one would not have to fulfil the requirements of the Directive, one could do whatever was agreed in the contract.

SPEAKERS' BIOGRAPHIES

BAKER, Michael	Michael Baker is the Executive director of the Asia Oceania Electronic Messaging Association (AOEMA) and has been an active member of the APEC Telecommunications Working Group (APEC TEL) since 1990. He was the inaugural chair of Standards Australia's EDI Committee in 1987, and the first CEO of the EDI Council of Australia. He wrote the initial constitution and rules for the Australia New Zealand EDIFACT board as well as serving on that group as a board member. He was also a board member of the EDI World Institute based in Canada and one of Australia's representatives on the International CALS Congress (based in the UK).
BAKER, Stewart A.	Stewart 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. Mr. Baker is a member of: the President's Export Council Subcommittee on Encryption; the Free Trade Area of the Americas Experts Committee on Electronic Commerce, and the UNCITRAL Group of Experts on Digital Signatures. He founded The State and Local Legal Center, which represents state and local government interests before the Supreme Court. Former Deputy General Counsel at the Education Department.
BAROUSKI, William	William Barouski is the Senior Vice President of the Information Technology Services department of the Federal Reserve Bank of Chicago, responsible for the overall function and direction of information technology solutions throughout the entire 7th Federal Reserve District. Prior to joining the Information Technology Services department, Bill was appointed Vice President of the Information Technology and Training and Education units of the Supervision and Regulation department. He joined the Federal Reserve Bank in 1980 as an examiner for the Supervision and Regulation department and in 1994, was assigned Vice President over all domestic banking.
BOULLE, Claude	Claude Boulle is Director, European Affairs, Groupe Bull, and chairman of EESSI (European Electronic Signature Standardisation Initiative). Mr. Boulle spent more than 20 years in Information Technology research and development and is a member of the HLSG -High Level Strategy Group for ICT- which brings together at European level representatives from the different

	industry sectors involved in the implementation of the Information Society. He has led several HLSG projects related to electronic commerce, including one dedicated to authentication and electronic signature
BOWDEN, Caspar (Intervenor)	Caspar Bowden is Director of the Foundation for Information Policy Research (www.fipr.org), an independent non-profit organisation which studies the interaction between information technology and society, identifies technical developments with significant social impact, and commissions research into public policy alternatives. Co-organiser of the Scrambling for Safety public conferences on UK cryptography policy, he was formerly an e-commerce and Internet security consultant, senior researcher of an option-arbitrage trading firm, a financial strategist with Goldman Sachs, and chief algorithm designer for a virtual reality software house.
BRANDEL, Roland	Roland Brandel is President of the American College of Consumer Financial Services Lawyers, and serves as co-chair of an annual national conference on the Emerging Law of Cyberbanking and Electronic Commerce. He has been active in bar association and community affairs. A former Chairman of the San Francisco Bank Attorneys' Association, he has served on or chaired numerous local, state, and national bar association groups and was a charter member of the Consumer Advisory Council, Federal Reserve Board. Mr. Brandel has served as a member of the Study Group on EFT of the Secretary of State's Advisory Committee on Private International Law.
BRIAT, Martine	Martine Briat is Director for banking co-operation, *Groupement des Cartes Bancaires* "CB", and an in-house lawyer since 1992. From 1985 to 1992, she was Director of the International Chamber of Commerce Institute for international Law and Practice, and from 1978 to 1985 Administrator in the Information, Computer and Communications Policy Division of the OECD, responsible for the legal programme of ICCP.
CHEE, Yeow Meng	Yeow Meng Chee is Assistant Director of the Internationalisation Office of the National Computer Board of Singapore. Yeow Meng's focus is on the development of national Public Key Infrastructures and Electronic Commerce Infrastructures, Cross-Certification, the formulation of Cryptography and Electronic Commerce policies in Singapore, and fostering international co-operation in Information and Communications Technology. He is Head of the Singapore Delegation to the ASEAN Coordination Committee on Electronic Commerce and OECD Committee for Information, Computer and Communications Policy. He also sits on the Management Committee of Netrust Pte Ltd, Southeast Asia's first Certification Authority. Yeow Meng is also a Fellow of the Institute of Combinatorics and its Applications and member of the International Association for Cryptologic Research.
DAVISON-JENKINS, Dominic	Dominic Davison-Jenkins is a Senior Vice President of FINPRO Advisory in New York. As an insurance broker and risk management consultant, he specialises in the identification and evaluation of complex risks, as well as the development of dedicated risk financing products. He provides risk advisory services to FINPRO clients and is involved in the development of innovative risk

	financing products (such as Net Secure for e-com-related risks). He is currently FINPRO National Practice Leader for both risk consulting and e-com/intellectual property. From 1991 to 1997 Dominic was a principal consultant with Minet Risk Services in New York City, specialising in all aspects of professional liability and intellectual property liability for U.S. and international organisations. Prior to this, he was a member of Minet's "Big 6" Accountants client service team in London.
DE BRISIS, Katarina	Katarina de Brisis works at the Ministry of Labour and Government Administration in Oslo, Norway, where she is senior adviser in the Department for strategic planning and coordination of information technology in the central government. She joined the Ministry in March 1998. Her special areas of responsibility include electronic commerce in public procurement, electronic administrative procedures, development of certification services and use of digital signatures in the public sector.
DRYDEN, John	John Dryden is Head of the OECD's Information, Computer and Communications Policy Division, Directorate for Science, Technology and Industry, since January 1993. He joined the Directorate in 1987, and has held a number of other positions, including Head of the EAS Division. Between 1980 and 1987, he worked in the Economics and Statistics Department of the OECD. Before joining the OECD, he worked in the Cabinet Office of the UK government.
ERBER-FALLER, Sigrun	Sigrun Erber-Faller is a lawyer, trained as a civil law notary. As an assistant manager of the German Federal Chamber of Notaries, he is in charge of European and International issues and all issues related to electronic legal transactions, with special focus on the legal effects of digital signatures and their use in provident judicial practice, especially in notarial practice.
FERGUSON, Peter	Peter Ferguson is Deputy Director-General of the Information Policy and Planning Branch, Industry Canada (IC) and a member of IC's Electronic Commerce Task Force. He is responsible for co-ordinating the development of policy positions on electronic commerce related issues such as privacy and security, access, digital signatures and certification authorities. From 1994 to 1997, Mr. Ferguson was a Director of the Secretariat for Canada's Information Highway Advisory Council, responsible for developing policy recommendations for the Council addressing a variety of information highway issues.
FIELD, Richard	Richard Field is an attorney in private practice, specialising in payment systems, electronic commerce and emerging technologies, as well as an Adjunct Professor of Electronic Finance at Columbia University Graduate School of Business. He is a member of the Council of the American Bar Association, Section of Science and Technology, and chairs its Electronic Commerce Payment Committee. He co-authored the ABA's Model EDI Payments Agreement (1992) and was a contributor to its Digital Signature Guidelines (1996). Mr. Field served on the US delegation to the United Nations Commission on International Trade Law,

	Working Group on Electronic Commerce. He assisted the European Parliament in its study of Electronic Payment Systems and Commerce, the Electronic Commerce Promotion Council of Japan in its studies of Certification Authorities, and the Korean Institute of Technology and the Law as an International Advisor.
FORD, Warwick	Warwick Ford is Chief Technology Officer at VeriSign, Inc., provider of public-key infrastructure solutions for e-commerce, enterprises, and the public. He is a recognized authority on the use of public-key technology, and led the development of digital certificate standards in ISO and the Internet community.
FOX, Barbara	Barbara Fox is Security Architect at Microsoft where she is currently responsible for the architecture of next-generation Web security. Her past projects have included Internet Explorer, Java, and most recently, the Windows 2000 public key infrastructure.
FUMY, Walter	Walter Fumy has worked at Siemens AG since 1986. His work involves cryptographic research, security consulting and participation in international security standards forums. For many years he has been active in the standardisation of security techniques, and is currently serving as vice-chairman of ETSI TC Security, and chairman of ISO/IEC JTC 1/SC 27 "IT Security Techniques".
GUIDA, Richard A.	Richard Guida joined the Treasury Department in October 1998 as a Senior Technical Advisor. Since 1998, he is a member of the Government Information Technology Services Board (Champion for Security) and Chair of the Federal Public Key Infrastructure Steering Committee. Commissioned as a naval officer, he joined the engineering staff of Admiral Hyman Rickover supporting the design and operation of nuclear powered warships. As a civilian, Richard assumed additional responsibilities within the Naval Nuclear Propulsion Program, culminating in 1988 with his selection as the Program's Associate Director for Regulatory Affairs and appointment in 1989 to the Senior Executive Service.
HIGASHIDA, Masanobu	Masanobu Higashida is responsible for R&D management in security at Nippon Telegraph and Telephone Corporation (NTT), which he joined in 1975. He is chairman of the InternetCash Experiment Promotion Group in the Foundation for Multi-Media Communication and since May 1996 is also a member of the Board of Trustees of both the Information Processing Society of Japan (IPSJ) and the Information Technology Standards Commission of Japan (ITSCJ). At NTT he initially worked on a proprietary computer hardware design project and since 1982, has worked on knowledge-based and natural language processing systems and their development.

HOUSELY, Russell	Russel Housely is Chief Scientist of SPYRUS and his expertise is in security protocols, system engineering, system security architectures, and product definition. He is the chairman of the IETF S/MIME Working Group and primary author of the Cryptographic Message Syntax (CMS). Rusell is one of the authors of the Internet X.509 Certificate Profile, commonly called PKIX Part 1, and of the SDNS Message Security Protocol (MSP), the security cornerstone of the Defense Message System (DMS).
INAGAKI, Fuminori	Fuminori Inagaki was assigned as Director, Information, Computer and Communications Planning Office at MITI in 1998. Since then, he has been involved in establishing policy and rules regarding promotion of informatisation and electronic commerce.
KATOH, Masanobu	Masanobu Katoh is General Manager of the Fujitsu Limited, Washington, D.C. Office. He is currently chairman of the private sector group Internet Law and Policy Forum (ILPF) and the chairman of the Work Group on Electronic Commerce for the Global Information Infrastructure Commission (GIIC). Mr. Katoh also participates in and represents the U.S.-Japan Business Council; the World Information Technology and Services Alliance (WITSA); the International Information Industry Congress (IIIC); the Japan Electronic Industry Development Association (JEIDA), and the Alliance for Global Business (AGB). He is a member of the U.S. State Department's Advisory Committee on International Communications and Information Policy, where he serves as co-chair of the Working Group on Intellectual Property, Standards, and Interoperability.
KAKULAVARAPU, Bhaskar	Bhaskar Kakulavarapu is Manager, Advanced Technology, Information Technology Department at Lear Corporation and for the last 5 years has worked on various strategic projects including Product Data Management, Remote Access, Internet Services, Network and Systems Architecture. He is currently very actively involved with Automotive Network eXchange® (ANX®), and represents Lear Corporation at ANX meetings. He also chairs the Security Technology Work Group (STWG) for ANX.
KENT, Dr. Stephen T.	Dr. Stephen Kent is Chief Scientist- Information Security, BBN Technologies, Director- Security Practice Center, GTE Internetworking, Chief Technical Officer, CyberTrust Solutions. He oversees information security activities within BBN Technology, and works with government and commercial clients, consulting on system security architecture issues. In this capacity he has acted as system architect in the design and development of several network security systems for the Department of Defense and served as principal investigator on a number of network security R&D projects for almost 20 years. He is Director of the SPC, monitoring all security-related aspects of the service offerings of GTE Internetworking Services. As CTO for CyberTrust Solutions, Dr. Kent provides strategic direction for this certification authority business. Stephen Kent presently co-chairs the Public Key Infrastructure Working Group and is a member of the editorial board of the journal *Computer Security*. He was a member of the Internet Architecture Board (1983-1994) and chaired the Privacy

	and Security Research Group of the Internet Research Task Force (1985-1998) and the Privacy Enhanced Mail (PEM) working group of the Internet Engineering Task Force (IETF) from 1990-1995.
KENNAIR, Bill	Bill Kennair is a Scrivener Notary in the City of London, practicing as a Civil Law Notary, but under the Common Law system. He is a member of the Information Security Committee of the Science & Technology Division of the American Bar Association, an officer of the Informatics Commission of the International Union of Latin Notaries (UINL), *chargé d'affaires* for the UINL to UNCITRAL, Chairman of the CyberNotary Association UK and Chairman of the Information Security Working Party in the Electronic Commerce Project of the International Chamber of Commerce.
KOBAYASHI, Yoshikazu	Yoshikazu Kobayashi has been Program Manager of Telecommunications Relations, IBM Japan Ltd. since 1991. He joined IBM Japan in 1970, and has been involved in the work for standardisation of Information Technologies and contributed to the work on Open Systems Interconnection, in particular, as the convenor of ISO/IEC JTC1/SC21/WG4 on OSI Management from 1986 to 1991. He is currently involved in INGECEP, an APEC project on Integrated Next Generation Electronic Commerce.
KUNER, Christopher	Christopher Kuner is a lawyer in the Brussels office of Morrison & Foerster LLP: the practice centres on electronic commerce and legal aspects of the Internet. He is a member of the Legal Advisory Board of Directorate General XIII of the European Commission, and of legal working groups on e-commerce issues of the International Chamber of Commerce (ICC) and the United Nations Commission on International Trade Law (UNCITRAL). He is also Vice-Chair of Committee R4 (Electronic Commerce) of the International Bar Association.
MCCULLAGH, Adrian	Adrian McCullagh is Director, Electronic Commerce, Gadens Lawyers with responsibility for Electronic Commerce activities on a national basis. He has advised both Government and Commerce on strategic planning, technical developments and legal implications of electronic commerce and the Internet. He has served on the Federal Attorney General's Electronic Commerce Expert Group, the National Public Key Infrastructure Group for DOCA, and Standards Australia IT12/4/1 Certification Authorities.
MITRAKAS, Andreas	Andreas Mitrakas is a senior legal consultant of GlobalSign, a European CA and provider of PKI products and services. A qualified attorney he participates in the ICC ETERMS WG. He is the author of numerous publications on IT law.
NILSSON, Dr. Hans	Hans Nilsson is Manager of Professional Services at iD2 Technologies in Stockholm. He was Science and Technology Attaché at the Swedish Embassy in Tokyo. Currently Hans Nilsson is project leader for the European Electronic Signature Standardisation Initiative.
NYHOLM, Jari	Jari Nyholm is IT Security Architect with responsibility for the security architecture in MeritaNordbanken in Sweden and Finland. He joined Nordbanken in 1991 and is responsible for the implementation of the PKI-solution. He began

	his IT-career at the Swedish National Taxboard in 1987, and moved to Hewlett Packard, Sweden, as Systems Manager responsible for HP´s internal computer systems.
ORLOWSKI, Steve	Steve Orlowski is Special Adviser, IT Security Policy in the Information and Security Law Division of the Australian Attorney-General's Department, where he focuses on the development and implementation of national and international policies and strategies for the security of information systems, including Australia's National Information Infrastructure. He is leader of the APEC Electronic Authentication Task Group and a member of a number of committees of the Standards Association of Australia dealing with IT security and electronic commerce issues. Steve Orlowski has been involved in a number of OECD activities including the Working Party on Information Security and Privacy and the Ad hoc Group of Experts on Cryptography Policy Guidelines.
PINCUS, Andrew J.	Andrew J. Pincus is General Counsel for the U.S. Department of Commerce since April 1997 and is the chief legal advisor for the Department. Beyond his legal responsibilities, Mr. Pincus also serves as a senior policy advisor for the Secretary and the Department on a broad range of domestic and international issues, including electronic commerce, international trade, telecommunications, intellectual property rights, environmental issues, export controls and technology. He was a partner at the Washington, DC law firm of Mayer, Brown & Platt from 1988 to 1997, where he focused on Supreme Court and appellate litigation and legislative policy. From 1984 to 1988, he was Assistant to the Solicitor General at the U.S. Department of Justice; and from 1982 to 1984, Mr. Pincus was an associate at the firm of Hughes, Hubbard & Reed in Washington, DC.
RADIN, Margaret Jane	Margaret-Jane Radin is co-director of the Stanford Program in Law, Science & Technology and spearheads the information science curriculum for the program. She teaches Electronic Commerce, Law and Business in Cyperspace, and intellectual property courses. She holds a chair at the law school (she is the William Benjamin Scott and Luna M. Scott Professor of Law).
REABURN, Norman	Norman Reaburn is Deputy Secretary in the Attorney-General's Department, where his responsibilities include the Programmes, Maintenance of Law, Order and Security, the Australian Protective Service, criminal law, drug law enforcement policy, counter terrorism co-ordination and infrastructure protection, Information Law and Security, including electronic commerce and privacy, court building services and the Office of Film and Literature Classification. He is the Chairman of the Departmental Audit Committee and a member of the Boards of Law Courts Ltd, the Australian Institute of Criminology, the National Criminal Statistics Unit and the National Criminal Courts Statistics Unit. He is also the Commonwealth representative on the Criminology Research Council. He is Chairman of the OECD Working Party on Information Security and Privacy and a former Chairman of the OECD Ad hoc Group of Experts on Cryptography Guidelines.

SAAPUNKI, Ari Arto	Ari Arto Saapunki is Special Adviser in the Population Register Centre, responsible for the technology of Finnish Electronic Identification. He is a Member of the European Electronic Signature Standardisation (EESSI) steering group and a member of the Nordic Self-Assessment Test (SAT) standardisation group. He previously worked in the Ministry of Interior, police department, as an IT-security chief of the Finnish police forces.
SCHLECHTER, Richard	Richard Schlechter is Lawyer, European Commission, Directorate General XIII (Information Society: Telecommunications, Market, Technologies – Innovation and Exploitation of Research). His responsibilities include EU-Policy in the field of electronic signatures and encryption and he is currently working on a proposal for a European Council and Parliament Directive on "A Community Framework for Electronic Signatures".
SINGH, Supriya	Supriya Singh is a Senior Research Fellow at the Centre for International Research on Communication and Information Technologies (CIRCIT) at RMIT University, Melbourne. She is a sociologist studying electronic commerce and the nature of money within its social and cross-cultural context. Her focus has been on how and why individual consumers and small businesses mix and match different communication channels and forms of payment.
SMITH, Brian W.	Brian W. Smith joined the law firm of Mayer, Brown & Platt in 1992 and is a member of the firm's Financial Regulatory and Electronic Commerce Practice Groups and chairs the Firm's Y2K Task Force. He serves on the Department of State's Advisory Committee on Private International Law, the International Chamber of Commerce's Working Party on Privacy and Data Protection as well as its Commission on Telecommunications and Information Technology and on the U.S. Council for International Business' Electronic Commerce Committee and its Working Group on Privacy and Transborder Data Flows.
SOQUAT Hubertus	Hubertus Soquat is a Senior Official in the German Federal Ministry of Economics and Technology, with responsibility for National and international (European Union, OECD and G8 affairs) relations in security on information technology. He is Head of the German Delegation to EU negotiations on a Directive on electronic signatures, and German representative at GATT/WTO Geneva international trade negotiations. Hubertus Soquat is also the former German representative at the Council of Europe (Eurimages: Film support scheme)

STOKES, Peter	Peter Stokes is Deputy Chief Operations Officer (Business Development) for Tradelink, where he has overall responsibility for all aspects of expanding the company's portfolio of electronic commerce offerings including the evaluation and design of new services and EDI messages, development of the transaction handling systems to support them, and enhancements to the relevant customer software products. He joined Tradelink in 1993 and has since led the technical development of Hong Kong, China's community electronic commerce network. He has played a major role in the design, development and implementation of Tradelink Shared EDI Facilities (SEDIF) platform which provides a secure EDI interface between Hong Kong, China's 70 000-strong import/export trading community and the Government.
WEIGELT, John	John Weigelt is IT Security Engineer with the Canadian Department of National Defence (DND) and is currently the Senior Technical Advisor for the Government of Canada PKI Task Force. He has implemented various national-level key management systems within the Department of National Defence and published several papers in the area of IT Security
WING, Paul K.	Paul K. Wing is head of information security for Scotiabank. He is responsible for all aspects of information security including governance, awareness programmes, system risk reviews, security strategy/architectures, security operations over high risk centralised systems, security quality assurance and occurrence investigation, and a security technology research function. In 1997 he led the implementation of two public-key infrastructures (PKI's); one to support internal users and a separate PKI to secure Internet-based customer service. Mr. Wing has served as Chairperson of both the Canadian Bankers Association (CBA) Data Security Committee and Interac Association Security Committee; "Canadian expert" and delegate to the International Organization for Standardisation (ISO) - Banking Security, Cryptography since 1985; liaison officer between the CBA and the Canadian Government on cryptographic security matters; a user representative "consultant" to the SWIFT on the USE project and currently eTrust; and a member of the Canadian Defence Security Advisory Board (DSAB) on "Information Operation" advising the Department of National Defence.

LIST OF PARTICIPANTS

Bai AKRIDGE
IBM Corporation

Joe ALHADEFF
ORACLE

Alan ANDERSON
AICPA

Goran AXELSSON
Swedish Agency for Administrative Development

Richard BACH
Department of Trade and Industry, United Kingdom

Michael BAKER
Asia Oceania Electronic Messaging Association (AOEMA)

Stewart BAKER
Steptoe & Johnson

William BAROUSKI
Federal Reserve Bank of Chicago

Michael S. BAUM
VeriSign, Inc.

Finn-Olaf BERG
Norway Post

Kjell BERGAN
CHOD Norway/SEC

Victor BOERSMA
Information Technology Association of Canada

Mark BOHANNON
Department of Commerce

Jay BOLTON
Pricewaterhouse Coopers

Doria BONHAM-YEAMAN
Florida International University

Robert BOOGAARD
Ministry of Finance, Netherlands

Janjaap BOS
DSEMCO

Claude BOULLE
Groupe Bull

Caspar BOWDEN
Foundation for Information Policy Research (FIPR)

David BRAIDWOOD
Royal Bank of Canada

Roland BRANDEL
Morrison & Foerster

Ulrik BRANDEN
Swedish Community for Electronic Commerce (GEA)

Martine BRIAT
Groupement Cartes Bancaires

Linda BROWN
Infineon

Anne CAINE
Australian Government Solicitor

Jean CANTRELL
Dun and Bradstreet

Anne CARBLANC
OECD/DSTI

Meng Yeow CHEE
National Computer Board

Per CHRISTOFFERSSON
Telia Promstor AB

Jenny CLIFT
UNCITRAL

Roger COCHETTI
IBM Corporation

Yves CUSTEAU
BCE Emergis

Richard DANGERFIELD
Charles Schwab and Co. Inc.

Dominic DAVISON-JENKINS
J&H Marsh & McLennan

Ruth DAY
Internet Law and Policy Forum (ILPF)

Katarina DE BRISIS
Royal Ministry of Labour and Government, Norway

Rayne DE GRUCHY
Australian Government Solicitor

Edgar R. De LANGE
Ministry of Transport and Public Works, Netherlands

Philippe DEGAVRE
Ministry of Economic Affairs, Belgium

Nanette DI TOSTO
CertCo

Katrina DOERFLER
Cisco Systems Inc.

Paula DOWNEY
Stanford Law School

John DRYDEN
OECD

Marina EKMAN
RSA Data Security

Jon ENGLUND
Information Technology Association of America

Sigrun ERBER-FALLER
Bundesnotarkammer

Deniz ERÖCAL
Business & Industry Advisory Committee to the OECD

Irwin ETTINGER
Citigroup

Carolyn EVANS
Qantas Airways Limited

Kim FAMIGLIETTI
Charles Schwab & Co

David FARES
USCIB

Peter FERGUSON
Industry Canada

Nuno FERNANDES
Instituto de Comunicações de Portugal

Richard FIELD
Attorney at Law

Robbert FISHER
Pricewaterhouse Coopers

Ken FITZPATRICK
IBM

Warwick FORD
Verisign

Alex FOWLER
Electronic Frontier Foundation

Barb FOX
Microsoft

Chuan-Hsun FU
Ministry of Finance, Chinese Taipei

Walter FUMY
Siemens AG

Beat GISLER
Ministry of Finance, Norway

Seung-Cheol GOH
Information Security Agency, Korea

Ruud GOUDRIAAN
ING Group

Jeanne GOULET
IBM Corporation

Christian GRABER
Swisskey, Ltd

Bill GRAHAM
Industry Canada

Richard GUIDA
PKI Steering Committee, US Government

Lauren HALL
Software and Information Industry Association

Stuart HAMILTON
Taxation Office, Australia

Masanobu HIGASHIDA
Advanced Telecommunication Research Institute

Gail HILDEBRAND
Consumers Union

Jeremy HILTON
JH Consulting

Mikito HIRATA
NEC USA, Inc.

Richard K. HITE
Visa International

Chuan-te HO
Research Development and Evaluation Commission

Ragnar HORNDAHL
Federation of Swedish Industries

Hirofumi HOTTA
NTT

Russ HOUSLEY
SPYRUS

Eric IANKELEVIC
CCIB

Tomoya ICHIMURA
Ministry of International Trade and Industry, Japan

Francesco IMPARATO
Lawyer

Fuminori INAGAKI
Ministry of International Trade and Industry, Japan

Takaya ISHIDA
Mitsubishi Electric Corporation

Victor IZQUIERDO LOYOLA
Ministry of Industry and Energy, Spain

Laurent JACQUES
Ministry of Justice, France

Eivind JAHREN
Ministry of Trade and Industry, Norway

Aruna JAYANTHI
APTECH

James JOHNSON
GIIC

Gunnar JONSSON
Johsson & Hall / Ministry of Commerce & Industry
Iceland

Frank JORISSEN
Utimaco Safeware

Rosa JULIA-BARCELO
Centre de Recherches Informatique

Bhaskar KAKULAVARAPU
Lear Corporation

Masanobuh KATOH
Fujitsu

Sergej KATUS
VNO-NCW

William KENNAIR
John Venn and Sons, Scrivener Notaries

Stephen T. KENT
BBN Technologies

Tom KERR
Internal Revenue Service, United States

Margaret KESHISHIAN
US Permanent Delegation to the OECD

Klaus J. KEUS
BSI/GISA

Tassaduk KHAN
Inland Revenue Board, Malaysia

David KING
PricewaterhouseCooper Technology Centre

Mikael KIVINIEMI
Ministry of Finance, Finland

Yoshikazu KOBAYASHI
IBM Japan Ltd

Jindrich KODL
Office for State Information Systems, Czech Republic

Friedrich KOENIG
Regulatory Authority for Telecommunications and Posts, Germany

Christopher KUNER
Morrison & Foerster

Kozo KURIYAMA
NEC Systems, Inc

Carl LANDAUER
Charles Schwab and Co. Inc.

Mark E. LEBLANC
Department of State, United States

Leonard LEE
National Computer Board, Singapore

Anne LEHOUCK
European Commission

Michael LIDDICK
America Online

Francisco LÓPEZ-CRESPO
Ministry of Public Administration, Spain

Francois LORRAIN
Infineon

John MAKARYSHYN
Telus

Lennart MALMSTRÖM
Sweden Post

Frank MARCH
Ministry of Commerce, New Zealand

Akira MATSUO
Chuo Audit Corporation

Maureen McCONNELL
BCE Emergis

Adrian McCULLAGH
Gadens Lawyers

Helen McDONALD
Industry Canada

Kate McGEE
Oracle Corporation

Lynn McNULTY
RSA Data Security

Gisela MEISTER
Giesecke and Derrient

Paul Eugen MERTES
Deutsche Telekom AG

John MEYER
Taxation Office, Australia

Toshiyuki MIYOSHI
Ministry of Posts and Telecommunications, Japan

Najirah MOHD
Inland Revenue Board, Malaysia

Karen MYERS
EDS

Taizo NAKATOMI
Ministry of International Trade and Industry, Japan

Mohammed NASRULLAH
Ministry of Transport and Public Works, Netherlands

Ganesh NATARAJAN
APTECH

Hans NILSSON
iD2 Technologies

Roger NOLL
Stanford University

Jens NØRVE
Ministry of Trade and Industry, Norway

Jari NYHOLM
Meritta Nordbanken

Brenden O'CONNOR
RSA Data Security

Brian O'HIGGINS
Entrust Technologies

Hans ÖJEMARK
National Post and Telecom Agency, Sweden

Steve ORLOWSKI
Attorney General's Dept., Australia

Jacques PANTIN
Certplus

Yong PARK
Information Security Agency, Korea

Janet PEARCE STENZEL
University of Southern California

Andreas MITRAKAS
Globalsign

Nancy PERKS
Microsoft Ltd

Pierre PERON
Revenue Canada

Lauri PESONEN
Setec OY (Ltd)

Teresa PETERS
OECD/DSTI

Deborah PIERCE
Electronic Frontier Foundation

Andrew PINCUS
Department of Commerce, United States

Reinhard POSCH
Technical University

Arno PUDER
Deutsche Telekom AG

Paul PUTLAND
British Telecom

Glen PYE
Nortel Networks

Margaret Jane RADIN
Stanford Law School

Birgir Már RAGNARSSON
Ministry of Commerce and Industry, Iceland

Liina RANNE
PricewaterhouseCoopers

Norman REABURN
Attorney General's Dept., Australia

André REISEN
Federal Ministry of the Interior, Germany

Christopher REISSNER
Federal Economic Chamber, Austria

Michael RICKUS
Internal Revenue Service, United States

Declan RIGNEY
Office of the Revenue Commissioners, Ireland

Mike ROBERTS
ICANN

Peter ROBINSON
USCIB

Fran ROONEY
Baltimore Technologies

Graeme ROSS
KPMG

Paolo ROSSINI
TELSY Elettronica e Telecommunicazioni S.p.A.

Ira RUBINSTEIN
Microsoft

Ari SAAPUNKI
Population Register Centre

Gareth SANSOM
Industry Canada

Richard SCHLECHTER
European Commission

Florence SCHMIDT-PARISET
Ministry of Justice, France

Wayne SCOTT
IBM Canada

Viktor SEIGE
APP CZECH

Lily SHUE
ISACA

Supriya SINGH
CIRCIT Brian W. SMITH
Mayer, Brown & Platt

Geoff SMITH
Department of Trade and Industry, United Kingdom

Violet SOCHAY
Revenue Canada

Antonius SOMMER
TUVIT GmbH

Hubertus SOQUAT
Federal Ministry of Economics and Technology, Germany

Lauge SORENSEN
IBM

Jan STALHANDSHE
Ministry of Industry, Employment and Communications, Sweden

Peter Hubert STOKES
Tradelink Electronic Commerce Limited

Bill TIGA TITA
World Chamber Consortium

Tony TORTORICE
PricewaterhouseCoopers

Ronald VAN DER LUIT
Ministry of Transport and Public Works, Netherlands

Christiaan VAN DER VALK
International Chamber of Commerce (ICC)

Patrick VAN EECKE
Ministry of Justice, Belgium

Harri VATANEN
Sonera Ltd

Lionel VODZISLAWSKY
Ministère de l'Economie, des Finances et de l'Industrie, France

Fred WALL
HM Customs and Excise, United Kingdom

Rickard WALLENTIN
Ministry of Industry, Employment and Communication, Sweden

Sanghan WANG
Ministry of Foreign Affairs and Trade, Korea

Clare WARDLE
UK Post Office

Satoshi WATANABE
Ministry of Finance, Japan

John WEIGELT
Treasury Board Secretariat, Canada

Robert WEIL
Revenue Canada

Sheryl WEINER
AICPA

Henk WILDEBOER
Phillips Int.

Paul WING
Scotiabank Mary WONG
Morrison & Foerster LLP

Peter WOOD
Ernst & Young

Simon WOODSIDE
HM Customs and Excise, United Kingdom

Takashi YAGI
Hitachi ltd.

Virginie YAICH
Service central de la sécurité des systèmes d'information, France

Eiichi YOSHIKAWA
NEC Corporation

Melek D. YÜCEL
Scientific & Technological Council of Turkey

Ed ZEITLER Charles Schwab

CASE STUDY MATERIALS

Brokat AG

Authentication and Security in Online Transactions

Brokat is a publicly traded company (AG) under German law with headquarters in Stuttgart, Germany. Founded in 1994 by five partners, Brokat has swiftly grown to over 300 employees, and has offices in many countries throughout the world. Brokat is the market leader for secure Internet banking software in Europe, and also has as customers many of the largest financial institutions in Asia and North America.

Brokat produces software for online transactions, which uses encryption and digital signatures to ensure the confidentiality, authenticity, and integrity of the data. The e-Services Platform Brokat Twister enable electronic business solutions such as e-banking, e-brokerage and e-payment to be deployed. Twister's secure Internet gateway, X*PRESSO, allows the transfer of Java applets from the server to the client, which are then used to re-encrypt the client's communications with the server.

This paper gives Brokat's vision of security in online transactions, in particular with regard to authentication. It is based on the security architecture of Brokat Twister, which allows diverse services and distribution channels to be administered with a high degree of flexibility.

Security Requirements

Secure online communication requires security on a number of different levels, including the following technical requirements:

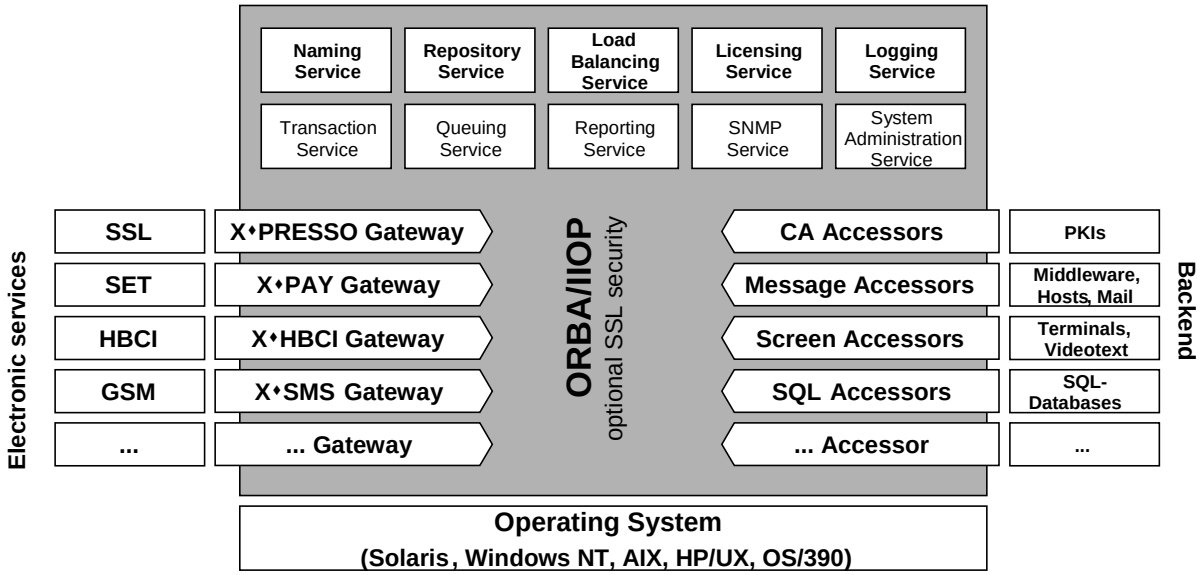
- Basic security (including elements such as confidentiality, integrity, and authenticity)
- Support of Standards
- Connection to existing security infrastructures
- Connectivity to heterogeneous systems
- Modularity
- Secure connection of distributed modules

Furthermore, there are a number of economic and political factors which must be present to enable truly secure online communication:

- Cost-effectiveness of security solutions
- Short time to market
- A flexible national and international legal environment (*e.g.* liberal encryption and electronic signature regulation)

SECURE AUTHENTICATION AND BROKAT TWISTER

The following explains how the above factors are realised in the context of BROKAT Twister. The basic concept of TWISTER is to combine functionalities existing in diverse back-end systems and to make them available electronically in different distribution channels.



TWISTER Architecture

The following are the elements allowing secure authentication in TWISTER:

- Secure External Channels. Twister supports secure communication in several networks and applications like Internet, GSM, OFX, and SET.
- External PKI connectivity. Twister can be connected to different public key infrastructures in order to support a wide variety of PKI implementations and policy infrastructures. For example, in Germany TWISTER can be used with the technical standard defined under the digital signature legislation, including the use of smart cards.
- Internal Security. TWISTER allows the optional use of SSL to achieve a secure communication channel between the Twister components.

Specific Authentication Applications

The following are a few of the authentication channels that can be accessed using TWISTER:

- Internet. Through X*PRESSO, TWISTER supports SSL connections over the Internet with mutual authentication and strong encryption.
- GSM. TWISTER allows secure authentication using digital signatures via the GSM mobile telephony standard. The required secret keys and algorithms are stored on the subscriber's SIM chip. Alternatively, the GSM channel can be used to transfer one-time-passwords for other channels, *e.g.* for Internet banking.

TWISTER also allows the use of other authentication mechanisms, including:

- PIN/TAN
- Hardware-Token
- HBCI
- SET

CONCLUSION

Security in online authentication requires flexible platforms such as TWISTER that can be quickly adapted to new technical, business and policy developments. Future developments that TWISTER will encompass include the use of new PKI systems and support for TLS (the successor to SSL). For mobile applications, support for elliptic curves and protocols such as WAP (Wireless Application Protocol) is also planned.

Contact:

BROKAT AG
Industriestraße 3
D - 70565 Stuttgart
Germany

Tel: +49-711-78844-0
Fax: +49-711-78844-777
E-mail: info@brokat.com

CLOUD COVER

PKI for Government

21 May 1999

Background

Communications-Electronics Security Group (CESG) is the UK's national authority for the technical aspects of Infosec. As such it has responsibility for setting national standards and policies for the security of electronic communications and information systems, and delivering Infosec products and services contracted for by Her Majesty's Government (HMG) and other authorised customers.

Introduction

CLOUD COVER is a CESG project which aims to set standards to foster the development by industry of Public Key Infrastructure (PKI) products and services to meet the electronic key distribution requirements of HMG. These products and services should be interoperable, cost effective and upgradeable. This will allow the progressive adoption of the HMG PKI by government departments at their own cost.

CLOUD COVER does not have the resources to install a pan-government infrastructure. Instead the aim is to stimulate the growth of an HMG PKI with a pilot implementation acting as the catalyst. CLOUD COVER will pilot a PKI on the main government intranet, known as the GSI (Government Secure Intranet). Security services will be provided to participants in the pilot scheme in a phased manner, starting with authentication and data integrity, to be followed by non-repudiation and confidentiality. Upon successful completion of the pilot other departments will be able to join the scheme at their own convenience.

Standards

The Architecture[1] recommended by CLOUD COVER is intended to make maximum use of open industry standards. The Architecture identifies the components expected in a PKI, their interactions and areas within a PKI where interoperability is an issue. For each area, the Architecture identifies the relevant standards that can be used and, where necessary, will provide guidance and clarification on their implementation and use.

The standards developed will be in the form of minimum specifications that constrain solutions as little as possible, but which place the emphasis on requirements covering: interoperability, functionality, assurance and preferred algorithms.

It is intended to validate these standards through the implementation and fielding of pilot systems, with a view to deployment in the GSI during 1999-2000. The pilots will use systems developed by Baltimore and Racal Research. These systems will be used as a reference model against which to compare implementations from other vendors.

Pilots

As a precursor to the main pilot CLOUD COVER has provided support to a NATO project, COAST II. COAST II (CRONOS Operational Assessment of Security Technologies) is aimed at piloting PKI technology to help NATO to establish its requirements for PKI and to establish the resource implications of running a PKI.

The COAST II project is a joint pilot between France, Germany and the United Kingdom to develop interoperable PKI and messaging systems. CESG has provided leadership for the trilateral pilot, and has developed client applications in collaboration with Compaq. CLOUD COVER has provided the necessary PKI standards and has developed a CA system under contract with Baltimore. When the systems have all been deployed, the project will have demonstrated interoperable solutions from three countries and at least five different developers.

To achieve this, the PKI has had to make use of very simple key management protocols and certificate profiles based on an early draft of RFC 2459 [2] and PKCS 10 [3]. Nevertheless, interoperability has proved difficult to achieve and shows the inherent problems in getting disparate implementations to interwork. However, simple as the COAST demonstrator is, it will provide a sound basis on which to build more complex, functionally rich, yet interoperable PKI systems. The success of the demonstrator has been shown by the willingness of other NATO nations to participate.

The COAST II pilot will be deployed to a number of users on an operational network. In addition to the considerations to enable interoperable PKI solutions, it is a further requirement that those who are involved with the pilot scheme can continue to communicate with those who are not.

The experience gained from COAST II project will be used in future phases of the CLOUD COVER project, in particular, the deployment of the pilot system to the GSI.

Further information on the work of CLOUD COVER can be found at http://www.cloudcover.gov.uk/

Contact:

E-mail: intl@cesg.gov.uk

REFERENCES

[1] CLOUD COVER Architecture, Issue 0.B, January 1999.
[2] Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile, March 1998, Internet Draft (work in progress).
[3] PKCS #10: Certification Request Standard, v1.0, November 1998, RSA Data Security, Inc. Public-Key Cryptography Standards (PCKS).

DIGITAL CERTIFICATION FOR CONSUMERS: THE EXPERIENCE OF GLOBALSIGN

Andreas Mitrakas
GlobalSign NV
Av. des Arts 1-2
1210 Brussels
Belgium.
andreas@globalsign.net
http://www.globalsign.net

Introduction

The rising demand for secure electronic transactions could not miss out the consumer market. The distinctive features of electronic commerce as opposed to former types of electronic transactions make services available to consumers as well as business. The legal environment in which digital certification services are offered will determine in the future consumer behaviour towards the application and the service providers.

Related projects

Much like electronic commerce transactions, digital certification is an activity that appeals mainly to business-to-business relations. Proof of that is GlobalSign's own record of transactions. In 1998, the bulk of certificates issued addressed business-to-business requirements at a rate of 70% followed by 20% for business to administration ones. Direct business to consumer related activities only covered 10% of GlobalSign activities in 1998. We must acknowledge, however, the impact that certain business-to-business or business-to-administration projects have on consumers.

Projects related to consumers have also been initiated in co-operation with two Internet service providers (ISP) to deliver digital certificates to consumers. The IBM Global Network and Planet Wallonie in Belgium both provide their customers with GlobalSign digital certificates. GlobalSign also encourages the widespread use of certificates by consumers by offering products that assure secure communications within consumer groups. The most challenging endeavour for the future, however, is Internet banking aiming at giving consumers the ability to communicate securely with their bank.

The electronic filing of social security declarations in Belgium is not an activity directly related to consumers. Speeding up the processing of submitted forms can have a direct impact on the service offered to citizens and this is achieved with the use of digital certificates. The same can be said for the secure transmissions among the members of the LEGANET user community. In an effort to assure confidential transmissions of electronic messages the network of the Belgian Bar offers certificates to their users in order to improve services to their clients.

Strategy

GlobalSign claims its role not just as a certification authority but also as the operator of a network of interrelated certification and registration authorities. By means of an expanded network GlobalSign is able to reach out to consumers residing in remote areas in the countries where it operates, in Europe and the Middle East.

It is also essential for GlobalSign to strive towards a branding policy that renders it recognisable as a distinct element of trust in the value chain and the consumer market. Branding can help the improving of consumer recognition and trust.

Policies

GlobalSign's policies are documented and published in a Certification Practice Statement (CPS), the contract binding GlobalSign and subscribers to certain legal terms and conditions. The GlobalSign CPS is available for consumer notice upon or before the registration of a subscriber and incorporated by reference in every certificate. Certification offers various levels of customer authentication that address different customer needs. Although contractual representations consumers are required to make vary according to the requested class of certificate, they include the following:

- The certificate applicant is the person identified in the request, subject to certificate class.
- The certificate applicant rightfully holds the private key corresponding to the public key to be published in the certificate.
- The information to be published in the certificate is accurate, except for non-verified subscriber information.
- Authentication procedures for consumers include the personal appearance of the applicant before a Registration Authority (RA) or a Local Registration Authority (LRA) in order to ascertain the link between the public key and the applicant of a certificate. Rejected applications are communicated to the applicant for their status. The applicant may retain his/her right to reapply for a certificate.

Following the issuance of the certificate, the subscriber makes the following representations to the certification authority:

- Digital signatures created using the private key corresponding to the public key published in the certificate is the digital signature of the subscriber. The certificate has been accepted and is valid at the time the digital signature is created. A valid certificate is the one that has not expired, been suspended or revoked.
- Unauthorised persons never had access to the subscriber's private key.
- The subscriber makes truthful representations to GlobalSign with respect to the information contained in the certificate. The subscriber must promptly notify the CA as soon as she has knowledge or notice of inaccuracies in such information.
- The certificate is issued for authorised and legal purposes as set out in the CPS.

After issuing a certificate GlobalSign additionally states to parties relying on a certificate that:

- Information in the certificate as well as information incorporated by reference therein is accurate, with prejudice only to non-verified subscriber information.
- GlobalSign has complied with the CPS when issuing the certificate.

In an effort to minimise incurring risks related to the core of its activities and cement trust in its network of RAs ands LRAs, GlobalSign offers a reasonable insurance scheme to consumers. According to this policy

GlobalSign bears all risks mitigating from the verification procedures in its entire network of RAs ands LRAs. It is also important to underline the second tier of the insurance scheme related to the possibility of compromising GlobalSign's own private key.

Legal requirements and concerns

Digital certification has been the subject of considerable regulatory legal work in Europe. The most recent token of this work is the Draft Directive on a common framework for electronic signatures (98/297). With respect to consumers and the legal position of GlobalSign we may note that GlobalSign, as a European CA complies with the European Directive on Data Protection (95/46). Further requirements the Directive imposes with respect to liability are as follows:

- The requirement to properly identify subscribers is firmly established through appropriate identification procedures backed up by an insurance scheme (art. 6.1.a).
- GlobalSign also complies with the requirements of this Directive (art. 6.1.b).
- GlobalSign obtains a contractual representation with regard to the assurance that the person identified in the qualified certificate held, at the time of the issuance of the certificate, the signature creation device corresponding to the signature verification device given or identified in the certificate (art. 6.1.c).
- GlobalSign sometimes indicates in the qualified certificate limits on the uses of a certain certificate, appropriately limiting its liability thereof (art. 6.3).
- GlobalSign also uses liability caps to limit the value of transactions for which a certificate is valid (art. 6.4).
- GlobalSign makes substantial efforts to provide notice to subscribers on the legal terms it uses for issuing its certificates.

Further incorporation of the Directive in the legal systems of the European Union member states will help create a more homogeneous market for certification services.

A direction for future action

As the demand for digital certification services grows it becomes increasingly necessary to facilitate the interoperability of certificates issued by the various CAs. It is essential to upgrade in-house drafted certification policies to the base material of industry-wide policies. CAs must be further encouraged to use commonly accepted technical standards and incorporate interoperability objectives in their practices.

Developing appropriate branding schemes is essential to the recognition of trusted services in online services. Branding may work better with new names that are not necessarily linked with already existing and known ones. The future holds the development of online business credentials appropriate for both consumers and businesses.

Further legal work is essential to maintain the current wave of regulatory reform in Europe and elsewhere to adapt legal systems to secure electronic commerce requirements. Issues like the incorporation of legal terms by reference are vital for the activities of CAs. Nevertheless, in a civil law jurisdiction this can be an issue of concern that is often neglected.

Conclusion

Electronic commerce is of direct interest to consumers. In spite of the slow growth as opposed to business or to administrative applications, consumers are able to use a variety of applications including digital signatures. A consumer friendly contractual policy as reflected in the CPS and enforced by appropriate insurance schemes, makes products for consumers legally safe to use. Further integration of the emerging legal rules into the national legislation is crucial for the upgrading of the legal safeguards for consumers. Future developments, however, are dependent on the further resolution of fundamental legal questions and the integration of interoperable technical standards in the applications.

The National Tax Board of Sweden and its Implementation of Electronic Signatures

The European Electronic Signature Standardisation Initiative
Brussels, Sodehotel la Woluwe
24 February 1999
Anders L Johansson

I will start with talking a little bit about what we have implemented so far, then I will go on an spend a little time on where we are heading in the near future and finally I will deal with some of the things we see as areas where sufficient solutions have yet to be presented.

Today we have a number of applications up and running that utilise electronic signatures. The electronic signatures we are using at this point are in-house produced and consist of smart cards (hard keys) as well as smart discs (soft keys). I will mention two of them:

- To enable companies to electronically communicate certain appendices to their tax returns, the National Tax Board has been distributing a smart disc called ELDA for a number of years. The software, certificate and secret key needed for this transaction is distributed free of charge to potential users.

- A newly developed case-handling system called MAGI, which stands for salestax and payroll tax, uses a smart card solution. Approximately 98% of the documents in MAGI are paper documents sent to the tax authorities as signed paper-originals which are scanned. The images are stored as TIFF-files.

Decisions, letters and other self-produced documents in the system are stored as electronic documents complete with electronic signatures. The documents produced in-house are also stored as TIFF-files.

The electronic signatures within the MAGI-application are created through the work-station's security-programme using MD5 and RSA. The signature is time-stamped by the National Tax Board's time-server by adding the time and signing the user's signature and the time-stamp as well as the time-server's identity using the time-server's private RSA-key. To store the document and the signature the signer must confirm that he or she wants to store the image as an electronic document. The MAGI-application then stores the electronic signature with the image.

* * *

Now a few words about how Swedish National Tax Board views the immediate future.

On behalf of the National Tax Board and several other central government authorities, *Statskontoret* is currently procuring frame aggrements for a platform for electronic communication (SHS - *spridnings- och hämtningssystem*).

[SLIDE: Yesterdays systems]

The implementation of this platform might be regarded as a giant technological step forward. Traditionally the different systems at the National Tax Board have been surrounded by distinct boundaries and, in a sense, re-inventing the wheel time and time again. This led to communications between the different systems being difficult at least, if not impossible.

[SLIDE: RSV Cityplan]

The new platform for communication will ensure more efficient electronic communication between authorities, companies and individuals, as well as simplifying the co-operation between public and private partners on the national level and within the EC. In doing so it will also facilitate processes that span over several authorities, for example the ambition is that this solution also will enable co-ordinated storage and re-use of basic information on companies.

When fully implemented the platform will enable electronic distribution of a vast variety of tax-returns via the Internet with electronic signatures.

The platform for communication will utilize open and preferably standardised technology. An example is that the XML-format is used as a label, or meta-data, to the information on its way from the signer to the recipient. Since the technical infrastructure of the National Tax Board spans over a spectrum of generations of technical platforms and solutions the XML-format for the information itself is not an alternative. Instead the file formats used depend on the destination application. Many of the systems we have today are too old to be cost-effeciently adapted to the format.

In parenthesis, I would like to mention that there is a project, initiated under the auspices of the Top Managers Forum called (freely translated) Electronic Case Handling, that will, among other things, look into issues regarding file formats for exchanging electronic documents within the Swedish public sector. The project is led by Mr. Torbjörn Hörnfeldt at the Swedish National Archives and is expected to present its findings before the end of 1999.

But to return to the topic at hand, the platform for communication will implement soft as well as hard keys. The ambition is to make use of certification service providers and commercially available smart-cards on the open market instead of depending on developing solutions in-house.

Parallel to this work *Statskontoret* is looking into the procurement of Certification Authority services comprising every step in handling the electronic ID-cards.

* * *

Since I am an archivist by profession the conclusion of this presentation might be easy to foresee.

One of the critical issues yet to be solved, we feel, is to be able to maintain authentic electronic documents with electronic signatures over time. It is not only a legal issue with the focus on the period of limitation, but also the necessity to ensure for tomorrow’s scholars the possibility to perform source-criticism on the documentation of today’s society.

Not only do the file formats become obsolete with time and demand migration of information and consequently re-signing, but the technology for electronic signatures itself will become obsolete and will require frequent re-signing.

Therefore a way to maintain electronic signatures including certificates, public and secret keys over time, with complete audit-trails must be found.

VeriSign Trust Network (VTN)

The VTN is a public key infrastructure that uniquely enables secure Internet-based electronic commerce. The VTN provides the necessary audit, security, and legal practices to facilitate a large, public, and widely distributed community of users with diverse needs for communications and information security. It leverages VeriSign's globally distributed root keys (which are embedded in all SSL-capable versions of Microsoft and Netscape browsers as well as over 40 Web server applications).

The VTN is operated by VeriSign in co-operation with its affiliates -- leading companies that are widely recognised, trustworthy technology providers from around the world, including: Roccade Magaplex (Netherlands), Comparex Holdings (Germany), British Telecom (UK), CertPlus/France Telecom (France), Acer/HiTrust (Chinese Taipei), AT&T (US), VSJ/NTT (Japan) and others. Additionally, over 700 leading ISPs and Web hosting companies are integrated into the VTN infrastructure.

The VTN has created an interoperable environment of online trust, as well as strong brand recognition. It supports various 'public' classes of Digital IDs where each class provides for a different level of trust. The VTN has also articulated a set of rigorous security and audit procedures for key management -- including root and issuing authority key generation, cryptographic hardware, and risk management services; and tailored E&O insurance and the Netsure Protection Plans (discussed below). The VTN consolidates a global public directory and certificate status publishing services. It is governed by the VTN Certificate Policy ("CP") document.

The proposed presentation will describe the VTN and its potential impact on the provision of globally secure Internet services – including the impact and interaction with government PKIs.

VeriSign NetSure(sm) Protection Plan

The NetSure Protection Plan is a pioneering and innovative warranty and insurance programme offered by VeriSign (and backed by the St. Paul Insurance Company) that provides enhanced protection against risks of transacting business on the Internet, including but not limited to:

- Loss, theft, unauthorised access of a subscriber's private key.
- Loss of use of a Digital ID caused by VeriSign-related services.
- Unauthorised revocation of a Digital ID.
- Delay or failure to request revocation of a Digital ID.
- Erroneous issuance of a Digital ID.
- Impersonation resulting from falsified information.

The protections offered by NetSure vary as a function of the class of certificate and other factors. For example, subscribers to Class 3 EDI certificates have an available aggregate certificate reliance limit of USD 250 000, and server certificate subscribers USD 200 000. Netsure is available for both US and

international customers. The NetSure Protection Plan will be available to VTN international affiliates on an optional basis.

The proposed presentation will introduce NetSure and consider its potential impact on future consumer protection regulation and risk management requirements for PKIs.

Who is VeriSign?

VeriSign, Inc. (Nasdaq: VRSN) is the leading provider of Internet-based trust services and digital certificate solutions enabling Web sites, enterprises, electronic commerce service providers and individuals to conduct trusted and secure electronic commerce and communications over IP networks. VeriSign provides diverse trustworthy PKI services – including the VeriSign Trust Network (discussed above). With more than 300 employees, VeriSign is rapidly expanding globally. VeriSign also supports over 100 000 Websites, 4 00 000 certificate holders, and more than 300 enterprises and government agencies. VeriSign has also enabled more than 150 ISV applications.

BACKGROUND MATERIALS

BACKGROUND PAPER ON ELECTRONIC AUTHENTICATION TECHNOLOGIES AND ISSUES

This background paper has been drafted for the Joint OECD-Private Sector Workshop on Electronic Authentication. It is intended as an input document for the workshop, to provide background information about electronic authentication technologies and issues in order to spark discussion about how these technologies work and the further potential for their use, and the role of authentication in electronic transactions. The initial draft of this paper was prepared by Stewart Baker and Matthew Yeo of Steptoe & Johnson, LLP in consultation with the OECD Secretariat; the paper has been revised by the Secretariat, taking into consideration comments received from members of the Working Party on Information Security and Privacy (WPISP).

I. Electronic commerce and communications and the need for authentication

Today's information networks and technologies are changing the ways that people communicate and do business, and they have a widespread impact on both the public and private sectors. A variety of electronic business transactions have been common for many years, but network technologies have generated an enormous potential for new kinds of electronic commerce. Exchanging information and conducting business over various types of information networks gives rise to a compelling need for methods of electronic authentication. [15] "Electronic authentication" can be understood to encompass any method of verifying some piece of information in an electronic environment, whether it is the identity of the author of a text or sender of a message, the authority of a person to enter into a particular kind of transaction, the security attributes of a hardware or software device, or any one of countless other pieces of information that someone may want to be able to confirm in the electronic world.

A closely related concept is an "electronic signature." Whereas the term "electronic authentication" refers to a technological method of confirming something about a piece of information, the term "electronic signature" generally refers to an identifier that is attached to, or logically associated with, an electronic message, document or data, and whose purpose implies the legal concept of a "signature" applied in the electronic world. In this sense, the term "electronic signature" reflects a legal implication when a particular technology is used to "sign" a message. An electronic signature could indicate a person's intention to endorse, approve, be bound by, or otherwise be associated with the contents of an electronic message, document or other type of data. However, in this legal approach, the electronic signature

15. It is relevant to recognise that user needs raised by the use of network technologies for electronic commerce and communications are not limited to electronic authentication. Users also require technologies and services to ensure the integrity, non-repudiation, confidentiality and secure storage of data. However, in accordance with the terms of reference for the workshop, this paper focuses only on electronic authentication.

technology need not necessarily, in and of itself, verify any particular piece of information, it need only indicate the signer's intent. For example, a typed name at the bottom of an e-mail message is one form of electronic signature -- albeit one with obvious security limitations -- if it indicates the signer's intent with regard to the text of the message. Where an electronic signature uses a particular method of electronic authentication to accomplish its legal goals, there is an overlap between the two concepts; since this is often the case, a comprehensive discussion of electronic authentication should also take into consideration issues related to electronic signatures.[16]

Questions for discussion

- What are the similarities and dissimilarities between traditional methods of authentication and electronic methods of authentication, particularly with regard to the environment in which they are used?

- Are there any parallels between the introduction of the electronic authentication and electronic signature methods being used today and the introduction of authentication or signature technologies used in the past?

II. The continuum of electronic authentication

A. Mechanisms for electronic authentication

As in the physical world, there are a wide range of methods that can be used in the electronic environment to confirm things about various aspects of some piece of information. At the simplest level, one can imagine a great many situations in which the parties to a communication or transaction can reasonably establish what they want to know about some piece of information without the need to interpose an intermediary. An obvious example is when the communicating parties know each other in advance and, in their communications with each other, refer to matters that they have discussed in person, by telephone, or through some other channel of communication. Every day, people rely on e-mail to engage in precisely these sorts of communications. While a standard e-mail programme has none of the types of secure authentication features discussed below, the fact that one can associate an e-mail address with a particular person over a regular course of communications is, in many cases, a sufficient method of confirming that person's identity in subsequent communications (a very basic form of electronic authentication). If the parties agree, an e-mail message could also be sufficient to establish the person's intent to be bound by the content of the message (a very basic form of electronic signature).

A system built upon pre-existing relationships can also work to create an informal "web of trust" arrangement for developing trust among previously unknown communicating and transacting parties. Such a web of trust operates when identification information is validated from person to person or from organisation to organisation in the context of established relationships. In this way, confidence in electronic representations extends from parties who have a direct relationship with each other to those who do not; by relying on a third party with whom each person has a pre-existing direct relationship to "make

16. For a discussion of the imprecise and inconsistent use of the terms "electronic authentication", "electronic signature" and other related terminology, see the workshop background paper on "The use of terminology in policy and legal discussions related to authentication and certification", drafted by the OECD Secretariat with the assistance of Steptoe & Johnson LLP.

the introduction," the communicating parties can create a reasonable assurance that they are who they say they are (at least to the extent that they each trust the third party). This method is quite commonly used for exchanging e-mail addresses; e-mail directories are seldom consulted to confirm that the e-mail address used is truly connected with a particular individual or entity.[17] This method is also currently used to certify public cryptographic keys for exchange of encrypted data among personal acquaintances. As electronic commerce develops, this method is evolving into an important element of business relationships as well, particularly where businesses that trust other businesses extend that trust among their respective clients.

Despite their prevalence as means of authentication, both of the methods described above require some pre-existing relationship between the parties or with a third party, and are generally useful only for establishing someone's identity. As such, they may not address the widespread need in the electronic environment for methods of confirming a particular aspect of some piece of information other than a person's identity, or for establishing an aspect of some piece of information in communications and transactions between parties who have no pre-existing relationship with each other.

The nature of the electronic environment gives rise to a compelling need for methods of authentication that can fulfil these purposes. To begin with, the sheer ubiquity of the Internet and other widely distributed information networks guarantees that there will be many situations in which the parties to a communication have no pre-existing relationship that forms a basis for trust. Indeed, one of the great promises of information networks is their ability to bring together people and organisations that might not otherwise have had occasion to communicate and do business with each other. Moreover, open networks such as the Internet are a fertile environment for all kinds of fraudulent behaviour, even though the reported instances of such fraud are relatively small. Transactions take place at a distance without the benefit of physical clues that permit identification, making impersonation easy. The ability to make perfect copies and undetectable alterations of digitised data complicates the matter. Knowing how simple it is to forge an e-mail, to alter the digital version of an agreement, or to create a professional-looking World Wide Web (WWW) page with no substance behind it can lead businesses and consumers to doubt that what they see is really what they will get on the Internet.

Technological solutions can be used in the electronic environment to overcome these basic obstacles to establishing identity and other attributes of communicating and transacting parties. While the manner in which these technologies operate will vary, their basic goal is the same: to bind a particular piece of information (such as someone's name and address) to another piece of information that is more susceptible to electronic verification (such as a password, a cryptographic key, or a piece of biometric information), such that the verification of the latter will confirm the truth or validity of the former. Often, the parties will require the interposition of some independent and mutually trusted entity that can confirm the relationship between these two pieces of information.

1. Public key cryptography for electronic authentication

The most widely-discussed of these technologies, and the one that has been most widely adopted to date, is "digital signature" technology. Digital signatures are based on a method of cryptography known as "public key" or "asymmetric" cryptography. Traditional methods of cryptography require some secure means by which the parties to an encrypted communication can exchange a single secret key in advance -- a method that is not readily adapted to open communications networks. Public key cryptography, by contrast, allows

---

17. E-mail addresses are also commonly accepted as a basic form of authentication when the domain name is trusted; for example, a correspondent who trusted that the OECD domain name indicates an OECD employee, would be likely to rely on an OECD e-mail address such as joe.smith@oecd.org.

parties to exchange encrypted data without communicating a shared secret key in advance. Rather than using a single key, public key cryptography uses two mathematically interrelated keys for each communicating party: a "public key" that is disclosed to the public, and a corresponding "private key" that is kept secret. A message that is encrypted with a public key can only be decrypted by the corresponding private key, and vice versa. It is this unique interrelationship that permits the creation of "digital signatures": if the sender of a message encrypts a message with his private key, and the recipient of the message is able to decrypt it using the corresponding public key, the recipient can be sure that the message could only have been sent by someone with control over the private key. By confirming that the corresponding public key "belongs" to a particular person or organisation, or is associated with some attribute, the receiving party can verify that information.

Digital signature technology can also be used to confirm that a document has not been altered in transit. If a document itself has been altered in any way after it has been encrypted with the private key, the digital signature will so demonstrate. Similarly, once a document is encrypted with the private key, the digital signature provides proof that the document was "signed" by the purported author, and the sender cannot easily deny having sent the document -- in this manner, digital signatures can function as a type of electronic signature. The same technology can be applied to ensuring the authenticity and integrity of documents archived electronically.

2. Biometric authentication

Another method of electronic authentication is based on biometrics. "Biometrics" refers to the use of innate human features, such as handwriting, fingerprints, voiceprints, or retinal scans, to confirm the identity of a person in an electronic environment. Depending on the use that is made of the biometric information, biometric technologies may require a trust infrastructure similar to that required for digital signatures to correlate a physical characteristic to a particular person or attribute of a person.

Biometrics are frequently used in conjunction with smart card technology. For example, a number of financial institutions have coupled biometric and smart card technologies in order to authenticate online banking customers. In such a system, a customer's online banking log-in, passcode, and fingerprint are stored on a chip which is attached to a multi-application smart card. An online banking customer places his finger on a scanning device attached to his PC. Computer software then matches the fingerprint image from the scanner against the image already stored on the smart card's chip.

Biometric systems may provide reliable authentication because it is difficult for one individual to fake the physical characteristics of another. On the other hand, forgery and compromise have long been recognised as threats to biometric authentication systems because if the physical reader can be bypassed and so that biometric data derived from scanning can be entered directly into the system, a person can be impersonated. Further, biometric devices may not always be reliable under abnormal condition (*e.g.* dirty fingers may bar biometric authentication based on fingerprints). Furthermore, the greatest obstacle to increased use of biometric authentication technology has been the cost of equipping terminals and workstations with the sophisticated hardware input devices that most biometric authentication techniques require. The cost of these devices is rapidly dropping, however, and several companies have announced plans to incorporate fingerprint readers into mass-market computer devices.

Questions for discussion

- What are the particular advantages and disadvantages of the different authentication technologies described above?

- What special policy issues, if any, are associated with each technology?
- Are there any other technologies currently used?

B. Certification authorities

Technological solutions for the various methods of electronic authentication among parties with no pre-existing relationship may be limited in application without accompanying certification mechanisms. The need for a reliable way to determine that certain information in the electronic world is verifiably connected to a transacting party can be filled by a new kind of intermediary -- a certification authority (CA) -- which acts as an independent trusted source to attest to some factual element of the information. In this way, certification authorities may become an essential supporting feature of technologies to enable electronic authentication. Generally, any public or private sector body (or possibly an individual) which reasonably inspires trust among the user community could act as a CA to independently confirm some aspect of a piece of information.[18] Certification authorities could utilise a variety of technologies to perform different functions in this regard. A CA could operate either "in-house" for an individual organisation or for the public at large.

It is important that the certification authority itself be reliable and trusted in order to inspire confidence in the information it certifies. Trust in CAs could arise from government involvement -- such as government licensing of CAs or a government agency which acts as a CA itself -- or it could arise from trusted private sector entities -- such as a business which provides certification services or a professional organisation that certifies information about its members. However, another element which may need to be considered is that the certifier will need to be certified. This issue could be addressed by both a hierarchy of certification authorities and a system of cross-certified certification authorities -- mechanisms which may be particularly relevant in an international context. However, the disparities between different government and industry views on the kinds of certification mechanisms that are being developed and the operational requirements for CAs may complicate the process of cross-certification; there may be a need for an internationally co-ordinated approach to outline base level criteria for cross-certification. The distinction between the informal mechanisms for building trust based on pre-existing relationships and more formal certification authority mechanisms becomes less clear when organisations which provide certification functions cross-certify one another.

To be effective, a CA must inspire the trust of transacting parties in the information that it certifies. Transacting parties must determine whether their level of confidence in certified information is proportional to the risk they are prepared to face if the information turns out to be false. In that context, they will need to consider the level of certification which is appropriate to their needs for a transaction and the degree of reliance they can place on information verified by a particular CA intermediary. In order to make an informed judgement, businesses and consumers should consider the certification authority's organisational, technological and procedural competencies, as well as the legal environment under which a CA operates. Additionally, the CA's procedures for verifying information and rendering certification

---

18. Recently, the term "certification authority" or "CA" has been interpreted to mean an entity which certifies public cryptographic keys; however, such a concept of certification authority could unnecessarily limit the potential for broad applications of certification mechanisms in the electronic environment. For the purposes of this paper, the term certification authority is applied to the broader concept of a public or private sector entity which acts as an independent trusted source for certifying many kinds of information in the electronic environment.

should be well established and publicly known -- in particular with regard to the criteria for certification, methods for registration, and revocation of certification -- so that users can be fully informed.

Questions for discussion

- What are the different ways in which a CA can generate the requisite trust among both its subscribers and people who rely on the information that it verifies?
- Under what circumstances, if any, is there a need for governments to regulate or license CAs?
- What liability risks does a CA face? How can a CA manage those risks?

C. Types of information which could be authenticated

Electronic authentication technologies can be used to establish aspects of a great many different types of information, relating to people, organisations, and devices. One way to think about the types of information that can be authenticated is to consider two broad categories: identity and attributes. "Identity" encompasses information that is essential to understanding who or what a person, organisation, or machine "is," in some sense. In the case of a person, for example, this would ordinarily include the person's name, nationality, and perhaps other basic information such as place of residence. In the case of an organisation, it would ordinarily include the registered name of the organisation, the jurisdiction in which it is incorporated (if it is an incorporated entity) and its principal place of business. "Attributes" encompass virtually all other types of information, and can include such things as the authority of a person, organisation, or device to engage in some act, or the fact that a person, organisation, or devices adhere to certain standards.

It is important to distinguish among the different types of information that may be verified through the use of an authentication technology because, as discussed below, different legal and policy consequences are likely to flow from these applications.

1. Identity

The notion that an authentication technology can be used to confirm the "identity" of a natural or legal person, organisation, or device necessarily raises the question of what is meant by "identity."[19] Focusing on people, where identity is most likely to be a concern, we ordinarily care about who a person "is" in two different situations: when we want to have some means of holding a person accountable for their actions, and when we want to be able to rely upon a person's reputation.

The need for accountability arises in many different situations. Imagine, for example, that someone relies upon an electronic signature to enter into an online contract with an individual for that individual to provide a particular service. If the individual subsequently does not perform the service, the person relying on the electronic signature will want some means of identifying who the person is in the "real" world so

19. Exactly what is meant by "identity" is an interesting question. A name is purely an identifer, while other characteristics (age, hair colour, job title, etc.) are not in a strict sense, but they are so closely identified with an individual that it can be difficult to decide what is "identity" and what is an "attribute". This is a line of philosophical inquiry that can result in a fascinating -- if time consuming -- debate, but in the end it may not be immediately relevant to the task at hand.

that he or she can seek redress -- for example, by serving a judicial summons on that person. The government is also likely to have a need to authenticate peoples' identities, for example, in connection with filing tax documents or confirming an entitlement to government benefits.

A person's identity may also be significant if that person has a reputation or other unique trait that is relevant in a particular context. For example, the fact that a medical opinion was written by a physician with a well-known reputation in his/her field is likely to be significant to other physicians who read and rely upon that information. In that context, the identity of the physician matters. The same physician, however, may use an online system to prescribe a medication for a patient, and the pharmacy receiving the prescription is only interested in whether the message was sent by a licensed physician. In that context, the identity of the physician is not particularly relevant; it is the status as a licensed physician (an "attribute") that matters.

An important question about the use of authentication technologies to establish identity is whether the government is uniquely qualified to issue certificates for this purpose. By and large, most "general purpose" forms of non-electronic identification -- passports, driver's licenses, national identification cards, etc. -- are issued by national governments to their citizens. There are few, if any, examples of privately issued forms of personal identification that are readily accepted outside of a particular context. Significantly, some governments are already developing plans to issue general identity certificates. For example, several governments plan to issue digital identity certificates to their citizens for purposes of identification. The government will serve as a certificate authority and will set security standards for government-issued identification certificates. These certificates will authenticate core "identity" features such as the bearer's name, age, citizenship, and address, which can then be used for a variety of purposes.

From the government's standpoint, the most valuable use of these types of "identity" certificates may be to authenticate communications between the government and its citizens -- for example, in filing tax documents and managing entitlements. As in the non-electronic world, however, it will likely be the case that individuals will also use their government-issued identity certificates in private-sector transactions where identity is relevant for some reason. Furthermore, once an individual possesses a government-issued identity certificate, the individual may also use that certificate to obtain more limited "attribute" certificates within the private sector. (For example, a person could open an online bank account with the government-issued identity certificate and thereafter obtain a certificate from the bank that authenticates that person's banking privileges without necessarily revealing that person's identity to transacting parties.)

While the government generally has a monopoly on general-purpose forms of identification in the non-electronic world, there are, in fact, some private-sector entities that are either offering general identity certificates or are planning to do so. Depending on the underlying requirements for obtaining such a certificate, it may or not be a true surrogate for a government-issued identity certificate. For example, one kind of basic level certificate which is easily obtainable online merely authenticates the relationship between a key pair and a person who supplied a particular e-mail address at the time of registering for the service -- it cannot truly be said to authenticate a person's "identity." Several private-sector CAs also offer more robust identity certificates that require additional forms of proof -- for example, appearing at an established and reliable institution, such as a bank, and presenting some form of identification. At that point, however, the CA is likely to be relying on traditional forms of government-issued identification to confirm a person's identity.

2. Attributes

An attribute is a particular trait, or characteristic, of an individual, organisation, or device. While the universe of possible "attributes" is virtually limitless, the most important categories of attributes relate to authority, standards, and transactional information.

(a) Authority

"Authority" is one kind of attribute that encompasses any situation in which an authentication technology is used to attest to the fact that a person or organisation is authorised to do something, such as sign a contract on behalf of a company, spend money from a given account, or undertake a licensed or regulated activity. Such authorisation information may or may not be connected to identity. This type of authentication could have applications for anonymous purchases where a merchant does not need to know the identity of the consumer as long as it is possible to verify that the consumer is authorised to make a payment (as with a credit card purchase). Another way that it could be used might be to indicate that a party is authorised or licensed to engage in a particular kind of transaction, such as verifying a valid driver's license for online approval of a car rental agreement, or verifying a pharmaceutical license that would allow a company to purchase or distribute a drug. This type of authentication could also play a role in managing intellectual property rights, by verifying that a person or organisation is authorised to use, distribute, or copy a digital work.

(b) Standards

Another type of attribute that could be authenticated would prove that an individual or entity is in compliance with certain specified standards or legal requirements. This authentication could verify that the company adheres to a particular code of commercial practice, or that it meets certain requirements for security and privacy standards in the way it handles data that it receives. This type of authentication could also be used to cover Internet-based professional activities, verifying that a particular professional service offered in the electronic environment -- such as educational services or telemedicine -- meet certain professional standards or legal requirements. Such authentication could be displayed as an icon which would appear on a WWW page to indicate the standards or legal requirements with which the individual or entity is in compliance and link to another site for more information on what the authentication means. It could also be included in the header of a Webpage to be read by the user's Internet browser and automatically checked for compliance with the user's pre-set preferences.

(c) Transactional information

Information about a particular transaction is another type of attribute that could be authenticated, for instance for record-keeping purposes or as part of a notary service to prove certain characteristics of an "original" digital document. This type of authentication would confirm the fixed content of a document (attesting to data integrity), the fixed date and time of a document, (time stamping or read receipt), or the fixed location of a document (either in terms of location of transacting parties at the time of the agreement, or for purposes of archiving copies for future use). Authentication of this type of information could be used to meet the formality requirements for contracts as an electronic notary service; an electronic notary system would authenticate a contract or other document that was prepared electronically by a specific person on a fixed date, and it would create an electronic record of the event that would be archived for evidentiary purposes later on.

3. Devices

An altogether different type of authentication, but one that is extremely important, is device authentication. Authentication technologies may be used to establish that a particular piece of hardware or software has certain attributes, such as the right to access a closed network or to engage in secure communications. Authentication technologies are also likely to be important in the design of copyright-management systems, for example, in controlling whether or not information in digital form (software, music, video, etc.) can be duplicated. These applications have no direct relationship to authenticating a person's identity or attributes, but may yet prove to be the most pervasive application of authentication technology.

Secure Sockets Layer (SSL), the current standard for secure electronic transmissions, is today's most widely used computer-to-computer authentication method. SSL does not authenticate users. Rather, SSL relies on digital certificates to authenticate the server and the browser to each other, and to establish a secure communications channel between the two. Interestingly, SSL certificates account for the single largest number of certificates in use today.

Questions for discussion

- Are there any other categories or subcategories of information that can be authenticated?
- Who is in the best position to establish and authenticate the different categories of information described above?
- What are the different means by which a CA (or its agent) can initially establish the veracity of a piece of information that it intends to authenticate?
- What policy issues, if any, are associated with the authentication of the different categories of information described above?

D. Relationships between transacting and communicating parties

1. Transactions between parties with no pre-existing relationship

Much of the early interest in electronic signature technology arose from its ability to authenticate identity or other attributes in so-called "stranger-to-stranger" communications and transactions, *i.e.* communications in which the parties had no previous relationship with each other. In the context of the Internet and other networks in which previously unknown persons and organisations communicate and do business with each other, the ability to authenticate identity or some other attribute is valuable and important.

The use of electronic signature technology in this setting implicates an array of legal and policy issues that arise principally from the fact that the three parties to such a communication -- the sender, the recipient, and the authenticating Certification Authority -- have not necessarily had a prior opportunity to define their respective rights and responsibilities. Thus, when something goes wrong, the injured party's recourse is not always clearly defined. For example, if a third party relies on a message authenticated by a CA, and it later turns out that the identity or attribute authenticated by the CA was inaccurate in some respect that harmed the relying party, the relying party may seek to recover damages from the CA. However, in the absence of a pre-existing contract between the relying party and the CA, the law may or may not provide a cause of action or, if it does, the CA's potential liability may be so open-ended that it is unable to enter the

business. It is these types of problems that have motivated much of the legal and regulatory interest in electronic authentication systems.

Authentication systems aimed at transacting and communicating parties that do not have a pre-existing relationship try to address these challenges. For example, some systems attempt to address the problem of third-party reliance by developing an extensive certification practice statement for use in this type of authentication. In this case, the system seeks to bind relying parties to the terms of this certification practice statement at the time that the relying party authenticates a message. However, in the absence of established rights and obligations for keyholders, certification authorities, and relying parties, the challenges to the development of systems of authentication for parties with no contractual relationship are likely to persist.

2. Transactions between parties with a pre-existing contractual relationship

As the market for authentication technology has begun to emerge, it has become increasingly evident that many applications of authentication technology will occur among persons or organisations that have some pre-existing relationship with each other. Under these circumstances, the parties to the authenticated communication are able to define in advance their respective rights and responsibilities in respect of the use of that technology. Examples of these situations range from something as simple as a private agreement between two parties concerning the use and recognition of electronic signatures, to something as complex as a global network of persons and organisations who have all agreed to common terms and conditions for the use of electronic signatures. In the latter case, the parties' rights and responsibilities in respect of the use of electronic signatures may be defined not in a single agreement, but through a series of agreements among different parties to the system.

There are many examples of the use of authentication technologies according to predefined contractual relationships. SET, for example, is a method of secure payment that incorporates digital signature technology. SET relies on a series of agreements and rules among all of the participants to a transaction (*i.e.* the consumer, the merchant, the participating financial institutions, and the payment card company) to establish the terms and conditions for the use of that system. Another example of a large-scale system based on pre-existing relationships between parties is the recent announcement by eight major financial institutions that they intend to provide global authentication services, principally for use in international commercial transactions (*e.g.* to confirm the identity of international trading partners, or to authenticate trading documents). The participants' use of that system will be defined, again, by a series of operating agreements among the participating financial institutions and their clients who use this service. What these examples illustrate is that systems based on pre-existing contractual relationships need not be limited in membership; they can, in fact, seek to operate on a global basis and incorporate thousands or millions of participants.

One of the principal challenges facing these kinds of systems is the need to ensure that the parties' agreements concerning the use and recognition of electronic authentication methods are recognised and enforced in each jurisdiction in which the system operates. National laws and regulations may prescribe standards for the use of authentication technologies that conflict with the standards and usages established by contract. If national legislation does not permit parties to derogate from its requirements, parties to contractual system agreements may find that they are unable to enforce these agreements.

Questions for discussion

- For what kinds of transactions and communications is electronic authentication among parties with out a pre-existing relationship most likely to be used?

- What are the differences between systems that rely on a pre-existing contractual relationship among parties and those that do not? Do the two kinds of systems have different needs for government regulation?

- Are there any circumstances under which a private agreement concerning the use of an authentication method should not be given full effect under law?

III. Case study overview

This section discusses how electronic authentication technologies are being used, or are likely to be used, in everyday applications. The purpose of this overview is not only to help illustrate how authentication technologies are being used, but also to provide a practical context for consideration of the legal and policy issues associated with these uses. The overview of implementation models is divided into three sections: organisation to individual, organisation to organisation, and a "hybrid" category to capture financial and other professional services that serve both organisations and individuals.[20] Where possible, this overview highlights issues to be considered in the context of the workshop case study presentations and materials, and raises points about particular applications. The following set of questions provides a basic framework for examining the case studies.

Questions for discussion

- What technology does the authentication system use (*e.g.* digital signatures, biometrics, password protection)?

- What elements of information does the system authenticate (*e.g.* identity, authorisation, etc.)? Who is attesting to the various aspects of the information? How is the truth or validity of that information established in the first instance by the entity that attests to it?

- What use is made of the authenticated information by the person, organisation, or machine that receives the message or data?

- What legal consequences, if any, might flow from the use of the authentication technology? Is the use of the technology intended to bind one or more parties in any way?

- How are the rights and responsibilities of the various parties to the communication or transaction defined? How do the parties allocate any risks associated with the use of the authentication technology? What do they do if something goes wrong?

- Do the parties to the communication or transaction using the authentication mechanism have some pre-existing relationship with each other, whether directly or indirectly?

---

20. The suggestion was made that this paper should also look at the issues related to the use of electronic authentication for individual-to-individual communications. While this is recognised as an important point, the case study section is designed to follow the agenda of the workshop, to raise issues for consideration under each session. The workshop itself did not cover individual-to-individual communications, because it was focused on electronic commerce applications. However, authentication for individual-to-individual communications -- both in terms of communication among strangers and among users who are familiar to one anther -- may warrant further attention.

- Is the authentication system designed to be interoperable with other authentication systems?

- Is the authentication system intended to operate on an international basis? Are there any problems with its international operation?

A. Organisation-to-Individual

The organisation-to-individual category encompasses any situation in which an organisation, be it a corporate entity or a government entity, is using an authentication technology in communications or transactions with persons who are acting in their individual capacity, and not in connection with a trade or profession. As a general matter, this includes individuals in their capacities as consumers (with regard to companies) and as citizens (with regard to the government).

1. Business-to-Individual

It is useful to subdivide this category into business-to-individual applications and government-to-individual applications, and to focus, in the first instance, on the purpose for which the authentication technology is being used. Turning first to business-to-individual applications, the following examples illustrate some of the broad uses of authentication technologies that might be employed by companies:

- Loyalty schemes. One of the principal uses of authentication technologies in the business-to-individual setting may be to confirm an individual's participation in a "loyalty" scheme, and to whatever benefits flow from participation in that scheme. A loyalty scheme is generally any type of system by which a company rewards individuals for frequent patronage, whether by providing discounts or other benefits. The most common loyalty scheme, and one in which authentication technologies are already is use, is airline frequent flyer programmes. Several airlines have issued smart cards to frequent customers, which can be used for electronic ticketing, access to airport club rooms, and even, in some instances, for boarding the aircraft. Notably, the fact that a particular individual is a frequent customer is a fact that is known to the company itself, and the company will not ordinarily have to rely on third parties to establish or confirm this fact. Moreover, while the company may choose to keep track of loyalty customers by reference to the customer's name, many of these applications can be implemented without regard to a person's identity.

- Entitlement to goods and services. Companies may use authentication technologies as a means of confirming an individual's right to receive goods and services. For example, a provider of online information services could issue digital certificates to customers who had subscribed to the service, which the customer would then use to access the service. A digital certificate might also be used to confirm, for example, that an individual is a licensed user of a software application, and therefore entitled to install the application on his or her computer and, perhaps, to receive technical support and upgrades. Again, these are facts that are ordinarily known to the company, and that may or may not require knowledge of a person's identity to confirm.

- Age. Companies may rely on authentication technologies to confirm that an individual is old enough to purchase age-restricted goods and services (such as alcohol or adult items), or to access age-restricted Websites. Significantly, this is not a fact that can be independently established by the company or even by a private certificate authority (at least not without examining some form of government-issued identification).

- Identity. In some instances, a company may have reason to confirm a person's identity (name, nationality, and perhaps other basic information, such as address and national identification number), although these instances may, in practical application, be relatively few in number. While a company is ordinarily interested only in a person's attributes -- most notably, the individual's ability to pay for goods and services -- there are certain situations in which a company may want the ability to hold a person accountable for their actions (for example, when a person rents a car or agrees to abide by the terms of a software license). A company may also want to know a person's identity in order to confirm his prior payment either with that company or with a credit bureau. In other situations, the government may require the company to establish and record a person's identity prior to providing some good or service, such as opening a bank account, travelling on an aeroplane, or purchasing a firearm. In many of these instances, identity may need to be confirmed by reference to a government-issued form of identification.

The need for authentication in the business-to-individual context is not a one-way street -- there are many instances in which the consumer may want to confirm an aspect of some piece of information relating to a company. Examples include:

- Membership in "Seal" programmes. "Seal" programmes may be used to establish many different attributes of a company. A data protection seal, for example, might confirm that the company adheres to certain standards with regard to the protection of personal information; membership in such a programme could be confirmed through the use of a digital certificate issued by the organisation administering the program. Similarly, an authenticated seal might also establish that a company is a member of an organisation that sets general standards of commercial conduct, such as the Better Business Bureau.

- Confirming the identity or authority of employees. If the nature of a transaction requires direct communication with a purported employee of a company, the consumer may want the ability to confirm that person's affiliation with the company and, perhaps, his or her authority to engage in a particular course of conduct on its behalf.

2. Government-to-Individual

In contrast to the business-to-individual setting, where a person's non-identity attributes are ordinarily the chief concern, the government's principal purpose for using authentication technologies is likely to be to confirm a person's identity. A person's identity is of concern in a wide array of government applications, for example, in determining a person's entitlement to benefits and in accepting and processing electronic tax documents. It is worth noting that most of this kind of communication occurs within a country, where the government and the individual are governed by the national legal system and rules, so the international issues that arise in other situations may not be applicable here.

B. Organisation-to-Organisation

Many of the applications of authentication technology in the organisation-to-organisation context are the same as, or similar to, the applications of authentication technology in the organisation-to-individual context. As organisations, however, they are likely to have somewhat different concerns and emphases with regard to authenticating information. The following broad categories highlight some examples of the use of authentication technologies by organisations:

- Authority. One of the principal concerns of engaging in electronic transactions with another organisation will be to confirm the authority of the communicating party to act on behalf of that organisation. For example, the organisation may want to confirm that a communicating party is, in fact, an employee of the other organisation, or is authorised to make purchases or enter into contracts in the amount of the contemplated transaction. "Authority" could also encompass whether an individual or organisation is licensed to provide a regulated service, such as the practice of law or medicine.

- Trading or information networks. Authentication technologies are already being used in the organisation-to-organisation context to confirm the membership of organisations in large-scale trading or information networks. These networks can, for example, provide a basis for authenticated bidding and procurement systems, authenticated electronic data interchange systems, and systems for authenticating trade documents.

C. Hybrids: Financial and Other Business Services

Financial and other business services, such as law and accounting, are hybrids within this organisational framework, because they act in both an organisation-to-individual capacity and an organisation-to-organisation capacity. As such, the issues that the use of authentication technologies in this setting raise are somewhat crosscutting.

Focusing on financial service implementations, the following general categories are examples of the use of authentication technologies in this area:

- Authority. Perhaps the most significant use of authentication technology in any setting is its use as a method of authenticating a person or organisation's authority to make or receive payments using a particular payment method, such as a credit card. In order for electronic commerce to flourish, technology will need to provide secure methods of transferring value over open networks. To date, that purpose has largely been fulfilled by relying on SSL (described above) as a means of encrypting credit card numbers. Over time, however, companies will need to develop methods not only of protecting credit card numbers in transit, but also of authenticating a person's authority to make payments using that card.

  One such system is the Secure Electronic Transactions protocol (SET). Announced in 1996, SET is a technical standard for safeguarding payment card purchases made over open networks such as the Internet. SET supports World Wide Web transactions between sellers and buyers and also supports business-to-business transactions such as inventory payments. The SET protocol relies on digital signature technology to authenticate both merchants and cardholders. In accordance with the SET protocol, digital signatures and cardholder certificates are used to authenticate cardholder accounts, not the identity of the user. The SET system of authentication operates on the basis of a predetermined contractual agreement among parties. The rights and liabilities associated with SET (and the digital signature technology on which it is based) are allocated in accordance with existing contracts and credit card laws.

  Authentication technologies may also be used to verify the authority of a bank or other financial services customer to access his/her account online and to engage in financial transactions. Several banks are relying on authentication technologies to provide authenticated access to online financial services.

- Settlement and trading networks. Financial institutions are also relying on authentication technologies to develop authenticated methods of trading securities and settling payments. The U.S. Securities Industry Association, for example, is establishing the Securities Industry Root Certificate Authority as a means of authenticating securities-related transactions among members of the industry.

WRITTEN SIGNATURE REQUIREMENTS AND ELECTRONIC AUTHENTICATION: A COMPARATIVE PERSPECTIVE

Christopher Kuner[*], Morrison & Foerster LLP, Brussels
Anja Miedbrodt[**], University of Frankfurt-am-Main, Germany

SUMMARY

Differences in the definition of "written signature" are influencing the course of national and international policies on electronic authentication, as the examples of the US and Germany demonstrate. US law has gradually been reducing the scope of handwritten signature requirements, and places the greatest emphasis on respecting the intent of the parties. German law also respects party autonomy, but requires that certain transactions be concluded by a handwritten signature (meaning pen on paper), with no possibility for derogation by the parties.

These differences in the definition of "signature" in national law have found expression in electronic authentication policy. US digital signature laws are generally directed toward removing barriers to the acceptance of electronic authentication and toward reduction of evidentiary uncertainties. By contrast, the German Digital Signature Law does not deal with the legal status of electronic signatures, but instead sets forth a high-security technical standard, motivated by similarly stringent requirements for pen-on-paper signatures. It is therefore not surprising that policy makers frequently have quite different concepts in mind when they discuss electronic signatures.

The international nature of the Internet makes it imperative that national definitions of "signature" be harmonized as they relate to electronic authentication. This can best be done by understanding the changing role of written signatures, educating policy makers and governments, and developing an internationally-oriented definition of "signature". A basis for such a definition could be a scalable set of signature requirements based on the security needs of the particular application, such as whether electronic authentication was used to establish identity, to demonstrate a particular attribute of the signatory, or for some other purpose.

[*] ckuner@mofo.com.

[**] *Rechtsanwältin* and Research Assistant, Law Faculty of the University of Frankfurt, miedbrodt@yahoo.com.

I. Introduction

The growth of the Internet and its global nature are forcing governments to find common solutions to regulatory questions, which requires understanding of how different legal systems treat common problems. A good example is the drafting of electronic authentication[21] or electronic signature legislation. As a technology designed to enable seamless, secure communication on the Internet, electronic authentication requires a flexible, internationally oriented regulatory structure.

While there has been considerable regulatory activity concerning electronic authentication in recent years,[22] misunderstandings about the differing roles of written signatures in different legal systems have contributed to difficulties in implementing global rules. Taking US and German law as examples, this article examines differences in the legal definition of “signature” and their implications for the national and international regulation of electronic authentication.

II. The Function of written signatures

In considering the function of written signatures, it is important to distinguish between the concepts of a "writing" and of a "handwritten signature". In both the US and Germany, almost any perceivable evidence may be considered to be "written", including electronic evidence. However, "signature" is a legal term of art which involves application of the rules described below.

Broadly speaking, a handwritten signature is intended to fulfill a variety of formal functions, such as the following that are often cited in German legal literature:[23]

- Finality function (*Abchlußfunktion*). The signature should make it clear that the signed document represents a completed declaration of will, and not just a draft which the signatory did not intend to be bound by.
- Cautionary function (*Warnfunktion).* A signatory should be made aware that by his signature he is entering into a binding transaction.
- Evidentiary function (*Beweisfunktion*). A party should in case of dispute be able to use a signature for evidentiary purposes.

However, these functions are limited by a further important principle, namely that of party autonomy. That is, in most cases a signatory should be able to rely on an expression of his will (such as a signature) being respected and not invalidated by the legal system for failure to meet a handwriting requirement, as long as it is clear from the circumstances that he intended to be bound by it. The decisive question then becomes how a legal system balances these interests, which can be competing. For instance, respecting the will of parties who have agreed, *e.g.* that an "X" scratched onto tree bark is sufficient to convey a plot of land is

---

21. In this article, “electronic authentication” and “electronic signature” are used synonymously, with “digital signature” (using asymmetric cryptography) as a subset of “electronic signatures”. “Electronic authentication” may be understood as any sort of electronic verification of information, with “electronic signature” as a form of “electronic authentication” that indicates the intention to associate oneself *in a legal sense* with the contents of an electronic document.

22. See, *e.g.*, http://www.ilpf.org/digsig/survey.htm.

23. See Herda, *Elektronische Dokumente - Einführung in die rechtliche Problematik, in: Bundesnotarkammer* (ed.), *Elektronischer Rechtsverkehr* 37, 42-43 (Verlag Otto Schmidt 1995); *Palandt, Bürgerliches Gesetzbuch* § 125 Rdn. 1 (C.H. Beck Verlag , 57nd ed. 1998).

clearly in a state of tension with the need to provide clear evidence of ownership of real estate and to warn parties against entering into such important transactions too lightly. It is therefore not surprising that many legal systems make enhanced evidentiary privileges or even legal validity for certain transactions dependent on the fulfillment of handwritten signature requirements.

Achieving an appropriate balancing of these interests is more difficult when dealing with electronic authentication than in the case of traditional paper signatures. First of all, paper signatures have existed for thousands of years, while electronic authentication has only recently begun to be widely used. Thus, the experience that legal systems have built up regarding paper signatures is largely lacking with regard to electronic ones. Secondly, there is great uncertainty about how to balance the relative security risks of paper signatures versus those of electronic signatures. While it is clear that digital technology makes it possible to forge or manipulate electronic signatures on a scale impossible in the case of paper signatures, it is also clear that paper signatures have never been particularly secure, and that the same digital technology makes possible a degree of security unheard of in the case of paper signatures (*e.g.* through the use of encryption technologies). This has understandably led to uncertainty among users about whether electronic signatures are secure or not, which has held back their broad acceptance.

III. Written signatures in the common law (United States)

While the United States is actually composed of 51 legal systems (50 states and the federal government), it is possible to generalise to some extent about written signature requirements. Generally speaking, contracts and obligations do not have to be in writing unless the law requires otherwise.[24] Other formal requirements in US law include the "contract under seal" and notarisation,[25] which, however, either have little practical importance nowadays (as in the case of the contract under seal), or are so easily satisfied that the justification for their continued existence is questionable (as in the case of notarisation, which in US legal practice generally means nothing more than having a secretary certify a signature upon request). As a signature can be any mark on a message made "with the present intention to authenticate" it,[26] in US law the emphasis is on whether the signer intended to be bound.[27]

In the US, questions concerning the validity of handwritten signatures tend to arise most frequently in the context of the so-called "Statute of Frauds", which is a remnant of the English common law that was incorporated into the Uniform Commercial Code that almost all US states have adopted. The Statute of Frauds provides that in order to be enforceable, certain types of contracts (such as those of a value more than USD 500) must be "in writing and signed by the party against whom the enforcement is sought".[28] Within this context, courts have held such indications of intent as a telegraphed name,[29] a fax,[30] and a telex[31] to be a "writing" or "signature". The key factors in the US decisions seem to be that, if the signature

---

24. See Smedinghoff (ed.), *Online Law* 83 (Prentice-Hall 1996).

25. See Perritt, *Law and the Information Superhighway* 386 (John Wiley & Sons 1996).

26. UCC § 1-201(39).

27. See *Online Law*, *supra* note 24, at 84.

28. UCC § 2-201(1).

29. Hillstrom v. Gosnay, 614 P.2d 466 (Mont. 1980).

30. Bazak International Corp. V. Mast Industries Inc., 73 N.Y.2d 113, 7 U.C.C. Rep. Serv. 2d 1380 (1989).

31. Joseph Denunzio Fruit Co. V. Crane, 79 F. Supp. 117 (S.D. Cal. 1948).

reflects the intent of the party, and it was recorded in a "tangible medium",[32] then it will be found to be a legally valid signature.[33] Signature and writing requirements are also found in other specific areas where there is a particular need for evidentiary certainty, such as regarding the filing of papers in court.[34]

The functions of a signature referred to above in the context of German law are by no means unknown to US law.[35] However, it is also clear that the trend has largely been away from written signature requirements.[36] US law emphasises the intent of the parties, rather than the security of the manner by which the signature is affixed, as long as certain minimum requirements (such as the use of a "tangible medium", which includes electronic media) are observed. Moreover, it is widely felt that the Statute of Frauds is no longer timely and should be repealed.[37]

Despite the generally liberal approach to the admissibility in court of electronic signatures, concerns about the acceptance of such evidence in practice have led almost all US jurisdictions to pass or at least seriously contemplate legislation intended to facilitate their admissibility.[38] While such legislation typically deals with much more than the evidentiary status of electronic signatures, the uncertainty caused by evidentiary disputes has been one of the major motivations in enacting US digital signature laws.[39]

IV. Written signatures in the civil law (Germany)

The German law of written signatures is complex and cannot be discussed here in all its permutations. However, it is possible to distill some general principles. Under German law there are no formal requirements for a contract to be valid, unless explicitly provided for by law, and it is possible for the parties to agree that a signature will have a particular evidentiary value. The vast majority of commercial transactions in German law do not require a particular form of handwritten signature, but such requirements do play a role in certain areas relevant to electronic commerce (*e.g.* in consumer credit transactions and in data protection law).[40]
German law contains five types of signature requirements:

- Those provided for by statute (*gesetzliche Schriftform*).[41]
- Agreement by the parties to apply statutory signature requirements (*gewillkürte Schriftform*).[42]

---

32. In this context, the use of an electronic medium (such as a computer display) which the user can use and read is considered "tangible".

33. Online Law, *supra* note 24, at 84.

34. See, *e.g.*, New York CPLR 2101(a), requiring with regard to court papers that "the writing shall be legible and in black ink".

35. See ABA Digital Signature Guidelines 3-4 (American Bar Association 1996), which refer (non-exclusively) to the following "general purposes" of a signature: evidence, ceremony, approval, and efficiency and logistics; Fuller, Consideration in Form, 41 Columbia Law Review 799, 800 (1941).

36. ABA Digital Signature Guidelines, *supra* note 35, at 5, note 10.

37. See Baum & Ford, Secure Electronic Commerce 44 (Prentice-Hall 1997).

38. See the list at http://www.perkinscoie.com/resource/ecomm/digsig/index.htm.

39. Baum & Ford, *supra* note 37, at 50 note 79.

40. There are over 3 000 written form requirements in German law.

41. § 126 Civil Code (*Bürgerliches Gesetzbuch* or BGB).

- Notarial[43] certification (*notarielle Beurkundung*).[44]
- Authentication (*öffentliche Beglaubigung*),[45] which is generally performed by a notary.
- Recordation in a protocol of declarations concerning a court settlement (*gerichtlicher Vergleich*),[46] which is used in place of notarial authentication.

Where a written signature is required by statute, the document has to be signed by hand by the issuer with his name or a handwritten mark which is authenticated by a notary.[47] Signatures by stamp,[48] typewriter,[49] or by telegram[50] or fax[51] are not considered to be "handwritten" in this context. The rationale for such statutory signature requirements is related to the functions of written form described above. For example, § 566 BGB requires that a lease of real estate longer than one year has to be signed by hand to provide evidence for the content of the contract,[52] while § 766 BGB provides that a surety bond requires a handwritten signature in order to warn the surety.[53]

When no statutory signature requirements are applicable but the parties have agreed to apply them anyway, the statutory provisions concerning signature requirements are applied unless the parties have agreed otherwise.[54] Thus, in this case the parties may derogate from the requirement of a handwritten signature, so that, for example, a transmission via telegraph between the parties would be sufficient.[55] In this case, the consequences of a failure to satisfy the agreed-upon formal requirements are determined by the agreement between the parties, so that whether or not the agreement is rendered void depends on the circumstances in each case.[56] By contrast, the failure to satisfy a signature requirement provided for by statute renders a transaction void in principle[57] (not just unenforceable), nor may the parties derogate from the legal rules concerning statutory form.[58] In some cases the failure to meet signature requirements may be counteracted, *e.g.* in the case of a conveyance of real estate by performance of the transfer and entry into the Land

---

42. § 127 BGB.

43. In civil law systems, notaries are highly-trained legal professionals, and are not comparable to US notaries public.

44. § 128 BGB.

45. § 129 BGB.

46. § 127a BGB.

47. § 126 BGB. There is controversy as to whether the signer can be represented by an agent.

48. BGH NJW 1970, 1078, 1080.

49. *Münchner Kommentar, Bürgerliches Gesetzbuch, Allgemeiner Teil* § 126 Rdn. 22 (C.H. Beck Verlag 1993).

50. BGHZ 24, 297, 302.

51. Palandt, *supra* note 23, § 126 Rdn. 7.

52. Palandt, *supra* note 23, § 566 Rdn. 1.

53. BGHZ 24, 297, 301. These two particular requirements do not apply to communications between "merchants" within the meaning of the Commercial Code (*Handelsgesetzbuch* or HGB); See § 350 HGB.

54. § 127 sentence 1 BGB.

55. § 127 sentence 2 BGB.

56. § 125 sentence 2 BGB.

57. § 125 sentence 1 BGB.

58. BGH NJW 1969, 1167, 1170, NJW 1973, 1455, 1456, NJW 1980, 451, 451.

Registry (*Grundbuch*),[59] or by performance of a gratuitous promise,[60] or by a surety performing the obligation in question.[61] But there is no general principle that the failure to satisfy signature requirements can be counteracted by performance.[62]

If notarial authentication (Beglaubigung) is required by statute (*e.g.* of a company registration[63]), the declaration in question must be in writing and the signature or the manual sign has to be attested by a notary,[64] who authenticates only that the signature is actually that of the signatory.[65] If notarial certification (Beurkundung) is required by statute (*e.g.* for a gift[66] or a conveyance of real estate[67]), the signatory will issue a written declaration to the notary, which will be read and approved; following this ceremony, the notary will sign the minutes.[68] Certification serves as proof that the declaration was issued in front of a notary, and replaces the legal requirement of a handwritten signature and notarial authentication.[69]

A written signature satisfying the formal rules described above enjoys enhanced evidentiary status under the Code of Civil Procedure (*Zivilprozeßordnung* or *ZPO*), so that it is presumed that the signed declaration was issued by the signatory.[70] The practical result is that parties often attempt to memorialise their understandings in a written document satisfying the formal requirements (called an *Urkunde*), in order to gain the benefit of these evidentiary presumptions. Because of the requirement of a handwritten signature and because of the lack of embodiment in a tangible medium, it is generally held that an electronic document cannot be an *Urkunde*,[71] meaning that it cannot enjoy the evidentiary presumptions described above. However, such evidence can still be admitted as "visual evidence" (*Augenscheinsbeweis*) or "expert evidence" (*Sachverständigenbeweis*), the weight of which is assessed by the court in its discretion.[72]

The capability of digital signatures to provide highly secure evidence of integrity and authenticity has made them the centre of attention in Germany to provide an electronic equivalent to written signature requirements. For instance, since 1990 it has been possible to submit an application for a default summons (*Mahnbescheid*) without a handwritten signature, if it is otherwise ensured that the application could not

---

59. § 313 sentence 2 BGB.

60. § 518 para. 2 BGB.

61. § 766 sentence 2 BGB.

62. *Brox, Allgemeiner Teil des Bürgerlichen Gesetzbuches 144, Rdn. 264* (20th ed. Carl Heymanns 1996).

63. § 12 HGB.

64. § 129 para. 1 BGB.

65. § 40 para. 1 of the Law on Certification (*Beurkundungsgesetz* or BeurkG)).

66. § 518 BGB.

67. § 313 BGB.

68. § 8 BeurkG.

69. § 126 para. 3, 129 para. 2 BGB.

70. §§ 440 para. 2, 416 ZPO.

71. Fritzsche & Maler, *Ausgewählte zivilrechtliche Probleme elektronisch signierter Willenserklärungen,* 1995 *Deutsche Notar-Zeitschrift [DNotZ]* 2, 19; *Mellius, Zum Regelungsbedarf bei der elektronischen Willenserklärung,* 1994 MDR 109, 112.

72. Roßnagel, *Die Sicherheitsvermutung des Signaturgesetzes,* 1998 NJW 3312, 3314; Bizer & Hammer, *Elektronisch signierte Dokumente als Beweismittel, 1993 DuD 619, 622.*

have been submitted without the intent of the applicant.[73] And in 1993 a law to expedite administrative procedures (*Registerverfahrenbeschleunigungsgesetz*) was amended to allow local authorities to maintain the Land, Company, and other registries in electronic form.[74]

On 1 August, 1997, the German Digital Signature Law[75] (*Signaturgesetz* or *SigG*) came into force. The Law is designed to establish general conditions under which digital signatures are to be deemed secure, and sets forth a voluntary technical standard which is intended to be secure for all applications.[76] Neither the Law nor the accompanying Digital Signature Ordinance (*Signaturverordnung* or *SigV*)[77] deal with the subject of handwritten signatures, as it was considered preferable to gather experience under the Law before providing legal equivalence between them and between electronic signatures.[78] The main legal innovation of the Digital Signature Law is that it provides that use of the technical standard defined by law will cause a digital signature to be "deemed secure",[79] although the exact effect of this presumption in German law is unclear.[80] There is no impediment to a court granting the same evidentiary value to other digital signature standards as to the statutory standard (for example, based on agreement by the parties); rather, the advantage at present to using the standard set forth under the Digital Signature Law is that users thereby enjoy a legal presumption without having to agree upon it in advance, which can also save costs by not requiring the court in each case to hear evidence about the security of the standard used. Additional legal advantages to using the statutory standard may arise in the future, as the government is presently examining the possibility of allowing fulfilment by electronic means of statutory signature requirements based upon use of the statutory digital signature standard.

V. Policy implications for electronic authentication

The differences in written signature requirements discussed above have already found expression in national and international policies on electronic authentication. For example, the German Digital Signature Law is based on a high security standard, which is at least partially due to the high level of security required to satisfy statutory signature requirements in German law and the intention to tie later relaxation of such requirements to the statutory digital signature standard. The connection between stringent written signature requirements and electronic signature regulation is also set forth in a German government paper on the "International Legal Recognition of Digital Signatures, which states in part: "In particular, a legal framework is necessary for the construction and erection of a (compatible) security infrastructure with a uniform organisational and technical security standard. The trustworthiness which is thereby attained offers

---

73. § 690 para. 3 ZPO.

74. *Gesetz zur Vereinfachung und Beschleunigung registerrechtlicher und anderer Verfahren (Registerverfahrensbeschleunigungsgesetz),* BGBl I, 1993, 2181-2235.

75. BGBl. I 1997, 1870, http://www.iid.de/iukdg/.

76. § 1, para. 1 SigG.

77. October 8, 1997, http://www.iid.de/iukdg/.

78. The German Federal Justice Ministry is presently examining electronic signatures and is considering amendments to existing laws to improve their legal status.

79. § 1(1) SigG.

80. See on this point Mertes, *Gesetz und Verordnung zur digitalen Signatur – Bewegung auf der Datenautobahn,* 1996 CR 7; Roßnagel, *Die Sicherheitsvermutung des Signaturgesetzes,* 1998 NJW 3312.

the possibility of ... legally allowing a 'digital form' with digital signature as the equivalent to 'written form' with a handwritten signature."[81]

Another example is provided by Article 9 of the "Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market" (the "E-Commerce Directive"),[82] which obligates the EU member states to ensure the validity of electronic contracts in their respective legal systems, but leaves the issue of meeting formal requirements (such as those requiring signatures) by electronic means to the proposed EU Directive on Electronic Signatures.[83] However, this latter Directive does not by itself provide harmonisation, since it does not apply to "non-contractual formalities requiring signatures".[84] The fact that both Directives in effect leave the harmonisation of written signature requirements to the member states indicates the sensitivity and difficulty of amending long-established written signature requirements in national law.

The US position, by contrast, has been based on principles that reflect the role of signatures in US law. For example, in early 1998 the US government proposed a "Draft International Convention on Electronic Transactions" to the Working Group on Electronic Commerce of the United Nations Commission on International Trade Law (UNCITRAL).[85] The terms of the proposed convention emphasise respecting the parties' agreement concerning the type of signature used, even to the extent of overriding applicable legislation.[86] US state and federal legislation on electronic signatures also generally reflects the view under US law that electronic signatures should be considered equivalent to paper-based signatures,[87] and that such equivalence should not be based on the security of electronic signatures.[88]

These examples suggest that differences in the definition of "signature" are already influencing the course of national and international policies on electronic authentication. In particular, common law lawyers often see written signature requirements as a formality that has been largely eliminated and remains only in a few isolated cases, while civil law lawyers often think of them in terms of security requirements that have a strong public policy aspect. Differing concepts of "signature" in the context of electronic authentication also seem influenced by the differing uses to which it is assumed this technology will be put, with US policy makers focusing on "low value" applications less concerned with identity (such as SSL certificates), while the German Digital Signature Law, by contrast, is based on a model that digital signatures will primarily be used to prove personal identity. It is therefore not surprising that policy makers from different

---

81. Draft of 28 August, 1998, available in translation at http://www.kuner.com.

82. 18.11.1998, COM(1998) 586 final.

83. COM (1998) 586, Annex commentary to Article 9. The text of the Directive was still being negotiated at the time this article was completed in April 1999; the original proposal of 13 May, 1998 is available at http://www.ispo.cec.be/eif/policy/com98297.html.

84. Article 1.

85. Available at http://www.un.or.at/uncitral/.

86. For instance, the section entitled "Party Autonomy" states that "The terms of any agreement (including closed systems) between parties governing their transaction should be enforced without regard to any statutory framework governing electronic authentication."

87. See, *e.g.*, Illinois Electronic Commerce Security Act, § 5-120, http://www.mbc.com/legis/ill-esca.html, which provides "Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law".

88. See *id.*, Comment 3: "It is important to note that while this section provides that any signature on an electronic record can meet statutory and regulatory signing requirements, it does not address the sufficiency, reliability, or authenticity of any such signature."

countries often seem to have completely different concepts in mind when discussing the definition of a “signature”.

There are clear dangers in dealing with a subject of such international importance in a purely national way. The international legal acceptance of authentication technologies will be impeded if each legal system clings to its own parochial conceptions of what constitutes a signature, which will also lead to increasing trade disputes and international tension. Moreover, useful regulatory activity in the area of electronic signatures (such as ensuring the removal of barriers to their legal validity) may become caught up in disagreements on the role of written signature requirements.

With all this in mind, it seems that the following considerations are of particular importance for policy makers as they grapple with regulating a technology that implicates widely differing concepts of written signatures:

- Understanding the changing role of written signatures. It is crucial that there be a realistic assessment by policy makers of the extent to which the functions of written signatures that have traditionally been recognized in national legal systems remain relevant in the context of electronic signatures. For example, while the "warning function" of written signatures remains an important value, one could ask whether it should retain its importance in the context of electronic signatures, or whether the fact that the Internet gives users an unprecedented degree of freedom and choice in the use of technology means that this function has lost much of its justification. Likewise, it is reasonable to ask that respect for the intent of the parties be evaluated in light of the extent to which complicated modern technology gives users a meaningful opportunity to understand the risks and benefits of using a particular signature technology.

- Education of governments. Experience has shown that, despite their best efforts, many policy makers dealing with electronic authentication often have a poor understanding of the technology, with the result that regulation in this area tends to be unrealistic and to lag behind the available technology. It is thus imperative that governments and international organisations concerned with electronic authentication take the time to learn about the technology and to avoid overly hasty regulation. Academia and the private sector can play an important role in assisting governments to better understand the technology and its economic and social implications.

- The necessity of an internationally oriented definition of “signature”. As the Internet brings national legal systems closer together, conflicts between them based on differing written signature requirements will become more and more likely. This argues for developing an internationally harmonised definition of written signatures, which would be based on a balance between ensuring security and respecting party autonomy. One might ask whether a definition could ever be found that would satisfy both competing values; an answer might be to develop a scalable set of signature requirements based on the security needs of the particular application. For instance, the definition of “signature” could differ if a means of electronic authentication was used to establish identity, to demonstrate a particular attribute of the signatory, or for some other purpose.

A first step toward such a differentiated set of definitions can be certain international standards which have already been adopted, such as Article 7(1)(b) of the 1996 UNCITRAL Model Law on Electronic Commerce, which defines the security standard an electronic signature must meet as a method "as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement". This in effect sets forth a "reasonableness" standard for written signatures, as it is based on the particular circumstances under which the signature is created and the uses to which it is put. Development of such a standard would have to take place on two levels: first of all, by amending national written signature requirements to bring them in line with the

requirements of the Internet age, and secondly, by continuing work on international agreements and policies.

Achieving increased appreciation of these factors is likely to be a long, drawn-out process, with the result that there will be tension between increasingly sophisticated electronic signature technology and legal rules based on centuries-old concepts of handwritten signatures. At the same time, there are signs that the potential exists for national written signature requirements to grow together over time. A number of jurisdictions seem to be following the path of granting basic legal validity to all types of electronic signatures, but at the same time of granting enhanced evidentiary privileges to signatures that meet certain minimum security requirements; this is the route taken, for example, in the German Digital Signature Law,[89] the Utah Digital Signature Act,[90] the Illinois Electronic Commerce Security Act,[91] and the UNCITRAL Draft Uniform Rules on Electronic Signatures.[92] However, closer examination shows the difficulty of harmonization even among such similar approaches. For example, even though the Illinois Act and the German Law both do not deny legal validity to electronic signatures that do not meet their respective statutory criteria, the Illinois Act allows the parties to determine the security techniques meeting the statutory criteria wholly by agreement, whereas the German Law sets them forth in great detail (though the parties can still derogate from them, at least to the extent that a statutory signature requirement is not involved).

What is becoming clear is that, whereas written signature requirements were earlier regarded purely as matters of national law, the growing use of the Internet and electronic signatures is putting increasing pressure on nationally-based conceptions of written signatures, and will force regulators and courts to confront the need to develop more internationally-oriented notions of the functions of a signature in a globally-networked world.

89. § 1(1) SigG.

90. § 406 Utah Digital Signature Act.

91. § 10-120 Illinois Electronic Commerce and Security Act.

92. Article 3, Version of 23 November 1998, A/CN.9/WG.IV/WP.79, http://www.un.or.at/uncitral/en-index.htm.

BUSINESS AND INDUSTRY
ADVISORY COMMITTEE
TO THE OECD

RECOMMENDATIONS ON AUTHENTICATION IN ELECTRONIC COMMERCE

This document prepared by the Alliance for Global Business (see page 7 about the AGB) is presented to the Joint OECD Private Sector Workshop on Electronic Authentication (Stanford and Menlo Park, 2-4 June 1999), as a minimum checklist of business requirements for government policies addressing authentication in electronic commerce. It contains a brief introduction on the status of authentication technologies and applicable terminology; a set of recommendations addressing government policies and clarifying business action; and suggested actions that business believes the OECD could take to further the market-driven development of authentication solutions to foster electronic commerce.

The recommendations in this document build on the high-level recommendations made by the AGB in its Global Action Plan for Electronic Commerce which was presented at the OECD Ottawa Ministerial Conference in October 1998. An updated edition of the Global Action Plan will be available in September 1999.

Introduction

Whether used for providing access to a corporate Intranet or for the identification of communicating or transacting parties (whether commercial or private), authentication techniques play an essential role in electronic commerce. Authentication of the parties to a transaction or communication, when properly carried out by reliable parties and/or through secure technology infrastructures, is a good method of building trust in electronic commerce.

As with all technology, authentication may be implemented at various levels of security and through a number of different technologies based on the requirements of the parties and the transaction or communication. For over 20 years, parties have used passwords and similar methods of authentication in EDI transactions. Today a continuum of technological approaches exists to help facilitate authentication across a variety of business models.

Among the most notable and secure technologies used for authentication are a variety of biometric and cryptographic "key-based" systems used as stand-alones, in combination, or as part of a larger technological solution. Of these technologies, many businesses believe that Public Key Infrastructure (PKI) based tools provide the most scalable solutions for commercially robust authentication available today. While recognising this fact, nothing herein should be read to be a disincentive to the development of new technologies or the application of other technologies which provide appropriate solutions. The following principles should facilitate implementation and deployment of any authenticating technology.

Terminology and technology neutrality

The term "authentication" refers to a large class of electronic applications whose functions may range from pure identification and authorisation to legal recognition. Referring to specific authentication techniques,

the terms “electronic signature” and “digital signature” are often used interchangeably. This has led to significant international confusion as to the use of the two terms. "Digital signature" is a functional subset of the more inclusive term "electronic signature". For the purpose of clarity, terminology used in this document shall refer to definitions with a certain level of international acceptance achieved through recognised international fora. The term “electronic signature” has been defined by UNCITRAL as “a signature in electronic form in, or attached to, or logically associated with, a data message, and used by or on behalf of a person with the intent to identify that person and to indicate that person’s approval of the contents of the data message.” Further, “digital signature” has been defined in ICC's General Usage for International Digitally Ensured Commerce (GUIDEC) as “a transformation of a message using an asymmetric cryptosystem such that a person having the ensured message and the ensurer’s public key can accurately determine: (a) whether the transformation was created using the private key that corresponds to the signer's public key, and (b) whether the signed message has been altered since the transformation was made.”

The distinction between electronic and digital signatures has been at the core of international discussions in recent years on whether policies should focus on electronic signatures or digital signatures. Government frameworks and policies surrounding authentication should facilitate the development and diffusion of existing authentication technologies and business models without disadvantaging emerging technologies. The AGB believes that in legal history there are many examples where different techniques for achieving the same end are facilitated through separate legal frameworks when these techniques reach the stage of commercial viability. It remains essential for governments to ensure non-discrimination. Governments should realise, however, that rulemaking is always limited by the existing terminology and technology to which it will be applied. The AGB believes that governments can and should continue work on international frameworks supporting the further growth of electronic commerce by promoting a liberal, yet predictable environment in which industry can continue to develop high quality, interoperable, market-driven solutions and standards for certification and authentication.

Recommendations

A. Policy principles

Policy approaches to authentication should foster flexibility and diverse business use of technology, practices, and procedures for all authentication tools in electronic commerce. The AGB recommends that such approaches should:

1. Promote Freedom of Contract

Freedom of contract can include, as appropriate, the following:

(A) Freedom of parties to agree contractually on the acceptance of electronically signed data and to agree contractually on the terms and conditions of transactions (including limitations of liability).

(B) Methodologies for enforcing online contracts and resolving disputes.

(C) Compelling public policy considerations such as public safety and prevention of fraud issues.

(D) Use of appropriate terms and conditions through incorporation by reference.

Promoting freedom of contract and maximising available technological and business choices allows parties to craft solutions to meet users' needs while still being supported by appropriate and predictable legal frameworks.

2. Promote technology neutral policies

Technology-Neutral Policies Permit the Diffusion of Current Technologies while Not Hindering the Development of New Technologies. Policies Concerning Authentication Should Be Separate And Distinct From Policies Regarding Confidentiality.

3. Address the continuum of authentication systems providing "architectural neutrality"

Policies should not dictate the type of architecture required for authentication. Policies should be architecturally neutral and enable different models to emerge to meet market demands.

4. Promote flexibility as to the content, form and function of certificates or authenticating mechanisms

Policies should be flexible to accommodate the diverse and changing market demands for authentication solutions. In particular, they should allow for certificates and similar devices to provide multiple levels of assurances of identity and/or any other user attributes, as required by market demand. Certificates and other devices used in authentication should conform to appropriate market-driven international standards to help provide commonality and to enable interoperability.

5. Promote Free and Fair Competition

Policies should not discriminate against authentication providers. Policies should promote free and fair competition among authentication service and product providers globally.

6. Enable A Predictable International Legal Framework for Authentication

Although at some later stage specific or sectoral rules for authentication may be required, there is an urgent need for generic operating principles for authentication at the international level. There should be market-based, non-discriminatory mechanisms for legal recognition of certificates and similar third party devices providing assurances of identity and/or other user attributes, as well as of the third parties themselves,

based on reasonable standards, without necessity of bi-lateral or multi-lateral agreements among independent sovereign states. Any regulatory procedures for recognition of certificates and similar third party devices providing assurances of identity and/or other user attributes should not be written to require local presence/partners or otherwise act as trade barriers. Neutral, objective, commercially reasonable and market-based criteria relating to adequacy should be used to determine recognition.

B. Business action

Business will continue to develop self-regulatory frameworks needed for authentication techniques to inter-operate internationally and to allocate equitably responsibilities among various parties to the transaction. Business continues to develop common definitions and best practice guidelines in the authentication and e-commerce arena.

Conclusion: role of the OECD

We recommend that the OECD could play a strong supporting role in the development of authentication techniques by agreeing to:

- Support implementation at the earliest possible time of the UNCITRAL Model Law on Electronic Commerce in all OECD Member countries.

- Recognise and support the benefits of choice and freedom of contract provided by allowing parties to determine the terms and conditions best suited to their transaction or communication.

- Appropriately support the UNCITRAL activity on electronic commerce, including its current work on electronic signatures, certification authorities and related legal issues.

- Catalogue, analyse and publicise how OECD Members countries implement the 1998 Ottawa Declaration on authentication.

- Recognise That Mandatory Licensing -- For Commercial and Non-Governmental Transactions - Of Certification Authorities and Other Third Parties Providing Assurances As To User Identity and/or Other User Attributes Will Impede Rather Than Benefit the Diffusion of Electronic Commerce across National Boundaries.

- Promote Education and Information Exchange on the Use of Market-Based Mechanisms of Recognition, and Especially Contracts, As A Basis of Providing For Legal Effectiveness or Validity of Messages Authenticated Using Commercially Reasonable Standards.

- Promote And Publicly Support Development Of Voluntary, Market-Based Standards And Private Sector Mechanisms For The Evaluation Of Third-Party Service Providers And Accreditation Criteria And Mechanisms.

About the Alliance for Global Business

The Alliance for Global Business (AGB, "the Alliance") is a co-ordinating mechanism of leading international business organisations created to provide private sector leadership on information society issues and electronic commerce. Jointly, these organisations represent the bulk of electronic commerce in almost all countries in the world. The coalition represents a diverse cross section of business in over 140 countries. Membership includes providers and users of information technology, large multinational enterprises and small start-ups, and companies in developing as well as developed economies.

The founding members of the Alliance are the:

- Business and Industry Advisory Committee to the OECD (BIAC).
- Global Information Infrastructure Commission (GIIC).
- International Chamber of Commerce (ICC).
- International Telecommunications Users Group (INTUG).
- World Information Technology and Services Alliance (WITSA).

The Alliance has issued a set of fundamental principles as the basis for policy making for electronic commerce. The Global Action Plan for Electronic Commerce, a living and evolving document, calls for minimal government regulation and emphasises business self-regulation as the most effective way of building confidence in transactions over open networks. The initial version of the plan was officially submitted to the OECD governments at the October 1998 OECD Ministerial Conference on Electronic Commerce. It sets out industry's views on the full range of e-commerce issues, including privacy, cryptography, consumer protection in the online environment, taxation of e-commerce, intellectual property protection, standards, competition and Internet governance.

The AGB Global Action Plan describes in detail business initiatives in all these fields so that governments are informed of the extent to which self-regulation is already operating and what further initiatives are under development. The plan's stated aim is to create trust in e-commerce across the whole spectrum of providers of services and goods.

In addition to describing specific business actions and commitments in the field of e-commerce, the plan identifies business expectations in regard to government action. Business would like to see governments concentrate on providing a minimalist and predictable legal framework in specific areas of government competence such as intellectual property protection, taxation, and the removal of barriers to competition in providing the underlying infrastructure. An annex to the action plan contained summaries of various business initiatives. Business executives who compiled the document said these provided ample evidence that comprehensive business self-regulation of electronic commerce is well on its way. The respective roles of government and business responsibilities need to be clarified, and that is what the action plan sets out to achieve. Furthermore, international organisations must ensure that their initiatives do not duplicate or contradict each other.

The Global Action Plan will be used by the Alliance to convey industry's views on electronic commerce in several fora in addition to the OECD. The coalition has issued a special adaptation of its Global Action Plan entitled "Trade-Related Issues in Electronic Commerce", which is being used in discussions with several other international organisations including the World Trade Organisation, the Asia Pacific Economic Co-operation (APEC) forum, the European Union, the Free Trade Area of the Americas, and others.

BIAC – Business and Industry Advisory Committee to the OECD

The Business and Industry Advisory Committee to the OECD (BIAC) is the voice of business from the economically advanced democratic nations of the world. Recognised by the OECD since 1962 as its business advisory counterpart, BIAC has the mission of ensuring that the OECD hears broad-based, considered business advice on all sectors of activity that it embarks upon. BIAC's membership consists of the principal industrial and employers' organisations of the OECD Member countries. These represent the majority in terms of employment, output, assets and investment by the private sector in the advanced market economies. Over the years BIAC, its member organisations, and their member companies have been deeply involved in the work of OECD on information and communications and electronic commerce, through direct participation in OECD committees as Observer and by providing technical and policy advice to various processes that develop OECD instruments such as the 1980 "Privacy Guidelines" or more recent work on cryptography policy.

GIIC - Forum for the Global Information Infrastructure

Launched in 1995, the Forum for the Global Information Infrastructure (GIIC) is a private sector advocacy group bringing together 50+ CEOs and Presidents of major international corporations with a stake in the development of the GII. GIIC members are from both developed and developing countries. The GIIC serves as a bridge between diverse players and business communities around the world, thus fostering the global dialogue necessary to address critical issues in building the global information infrastructure. The GIIC has established on-going policy dialogues with governments and international organisations, providing them with pragmatic advice and input as they transit to the new body of policies and laws needed to support a secure, seamless global communications environment and marketplace. Four main thrusts of GIIC activity are: 1) facilitating the creation of harmonised rules to support global electronic commerce; 2) bringing developing countries into the process of building the global information economy; 3) spurring the reform of education systems to prepare for the Information Age; and 4) fostering an open environment for the development of information infrastructure and services. GIIC membership is representative of all the major elements of the information technology sector, including telecommunications hardware and services providers, computer hardware and software companies, cable, broadcast, and publishing companies, new satellite companies, international organisations, governments, and academics. The GIIC's regional co-chairs are H. Brian Thompson, (Chairman and CEO of Universal Telecommunications), Volker Jung, (Executive Vice President, member of the managing board, Siemens), and Michio Naruto (Vice Chairman, Fujitsu). W. Bowman Cutter (Managing Director of E.M. Warburg Pincus) acts as the GIIC managing director.

ICC - International Chamber of Commerce

ICC is the world business organisation. With corporate and business organisation membership in more than 130 countries, it is the only representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world. Founded in 1919, ICC's purpose is to promote an open international trade and investment system and the market economy worldwide. Its rules for international trade transactions and trade finance are accepted globally by traders, governments and judges. The ICC International Court of Arbitration is the world's leading institution of its kind. ICC brings together executives and experts from all sectors of business to establish the business stance on broad issues of trade and investment policy as well as on vital technical or legal subjects. The ICC's broad framework of rules for international trade and commerce evolves continuously to take into account changes in business

practice. ICC has issued best practice rules for electronic commerce since the 1980s and continues to harmonise business rules and practices to meet the needs of the information society.

INTUG - International Telecommunication Users Group

INTUG is an international association of users of communications technology and applications. It has an extremely wide constituency. Founded in 1974, it has its Secretariat in Brussels where it is registered as an international non-profit organisation. It meets in plenary session four times a year. Members include national users groups which represent the interests of users in Europe, the Americas, Asia-Pacific and Africa. Associate and individual members come from major multinational enterprises, academia, law and other relevant industry sectors. Many of INTUG's member groups have been particularly successful in their interaction with national government policy makers; also in regional economic policy forums. INTUG itself promotes the interests of all users at the international level and ensures that the voice of the user is clearly heard whenever communications policy issues are addressed. Its Special Interest Group on Y2K issues has been extremely active and was a specific focus of the INTUG meeting in Brussels in June 1998.

WITSA - World Information Technology and Services Alliance

The World Information Technology and Services Alliance (WITSA) is a consortium of information technology industry associations from economies around the world. Serving as the global voice of the information technology industry, WITSA is dedicated to:

- Advocating policies that advance the industry's growth and development.
- Facilitating international trade and investment in information technology products and services.
- Providing members with a vast network of contacts in nearly every geographic region of the world.

WITSA:

- Serves as a forum for the identification of common issues and views.
- Formulates positions on information technology issues, including the recently concluded World Trade Organisation (WTO) Agreement on Basic Telecommunications Services.
- Voices the concerns of the international information technology community at multilateral organisations including the WTO, the World Intellectual Property Organisation (WIPO), the G-7 and other international fora where policies affecting industry interests are developed.
- Provides information on international marketing and business development.
- Promotes information sharing on information technology policy developments throughout the world.
- Hosts the biannual World Congress on Information Technology.

APEC TELECOMMUNICATIONS WORKING GROUP
BUSINESS FACILITATION STEERING GROUP
ELECTRONIC AUTHENTICATION TASK GROUP
ISSUES RELATING TO THE USE OF ELECTRONIC AUTHENTICATION

EXECUTIVE SUMMARY

In their 1998 Blueprint for Action[93], APEC Ministers recognised the enormous potential of electronic commerce to expand business opportunities, reduce costs, increase efficiency, improve the quality of life, and facilitate the greater participation of small business in global commerce. A cornerstone in achieving that potential is providing the tools that will allow parties to transactions to know with certainty the degree of reliance they can place on that transaction. Electronic authentication provides such tools through technologies that can ensure the authenticity of transactions. Some of the technologies also provide integrity, non-repudiation and confidentiality functions.

Electronic authentication is a developing field. As it evolves new technologies and new issues emerge. Addressing these issues is a problem for both users and government policy makers. This report identifies the major issues to provide APEC member economies with guidance when developing policies for electronic authentication. The report addresses the issues in general and is accompanied by technical annexes which examine four different groups of technologies and how these relate to the issues raised.

Definitions

There is a great degree of variation in definitions associated with both electronic commerce in general and electronic authentication in particular. There is a role for member economies to contribute to and stimulate international organisations' work in attempting to achieve the maximum degree of consistency.

Electronic business models

The Report examines a number of models of the environment in which electronic business might be conducted. These are provided to indicate the variety of different relationships that might exist between parties to an electronic transaction.

It also notes a trend towards requiring authentication in electronic transactions where signatures are not required in equivalent paper processes. It notes the potentially greater demands on and/or costs to businesses and users that can arise from this trend.

User requirements

User requirements cover technical, business process and legal requirements. It is recognised that these requirements need to be met in a consistent manner and a manner that is simple to operate and easy to

93. APEC Blueprint for Action, http://www.dfat.gov.au/apec/ecom/ecom_blueprint.html

understand. There is a role for both governments and business representative groups to ensure the requirements are met.

Electronic authentication technology

The Report discusses in broad terms the advantages and disadvantages of a number of technologies including implementations that involve the use of several technologies in a single transaction. These technology groupings will form the basis for the technical annexes.

It is recognised that different technologies can meet different requirements. The choice is one for the parties to a transaction based on a risk assessment. There is therefore, a need for governments to develop legal and policy frameworks to support all appropriate technologies.

Certification models

The report examines the different ways through which a recipient of a transaction can establish whether the claimed sender is the actual sender of an electronic transaction. As with business models, this information is provided to indicate the different relationships that might exist when trying to establish the authenticity of a transaction.

Trust

Trust can be achieved through the development of appropriate technology, development of appropriate legal and policy frameworks and development of appropriate business practices. Accreditation processes are designed to enable users to trust the technologies while legal frameworks are designed to enable users to trust that they can rely on the legal validity of a transaction. Awareness raising programmes are designed to build the level of required trust once the appropriate frameworks are in place.

Liability

Liability has been raised as one of the major issues facing users and authentication service providers. This issue is under active consideration in a number of international fora. Central to the discussion is whether governments should legislate in respect of liability or adopt a contractual approach. The issue is complicated by the fact that a number of economies are federations and jurisdiction for liability may rest with state or provincial governments.

It is likely that different jurisdictions will, at least initially, adopt different approaches. It will be important to ensure that adopting one approach does not prevent transactions with jurisdictions that adopt an alternative approach.

Roles of participants

As an essential part of electronic commerce, electronic authentication cuts across both the public and private sectors and extends down to individual users. For the electronic authentication schemes to function effectively, each of these groups needs to undertake defined roles. Examples of these are spelt out in the report.

Interoperability

The issue of interoperability means different things to different people. It has been argued in some quarters that we should be aiming for a single globally interoperable scheme. Others support the concept of a number of globally interoperable schemes. Different technologies will meet different requirements based on risk, cost and integration with other technologies. It is unlikely that the differing requirements can be met by a single scheme without compromising risk at one end or cost at the other. However too many schemes will confuse users, possibly increase costs as users need to implement an excessive number of schemes and leave users with a bewildering array of technologies attached to their systems. The objective should be to minimise the burden on users in order to encourage them to adopt electronic authentication and electronic commerce. Government and industry need to pursue an appropriate balance in consultation.

Technical standards and legal and policy frameworks will all impact on interoperability and cross border recognition of electronic transactions.

Accreditation

One of the main issues to be addressed is whether government should license or regulate authentication technology or authentication service providers. Approaches could include government licensing, government endorsed accreditation schemes, standards based accreditation schemes and industry endorsed accreditation schemes. Implementation of these schemes can be mandatory or voluntary. The type of approach adopted will vary from jurisdiction to jurisdiction determined largely by domestic policy on issues such as industry regulation and consumer protection. Problems will emerge if jurisdictions insist that authentication technologies or service providers satisfy their licensing or accreditation processes and requirements even where the service provider or user of the technology is located outside their immediate jurisdiction.

Cultural differences

The Task Group discovered several examples of cultural differences that have the potential to impact on electronic authentication. These highlight the need for governments to be sensitive to the existence of cultural differences between economies. Cultural differences have the potential to impact on technical, legal and policy aspects of electronic authentication. Often cultural differences are not addressed in these aspects through ignorance rather than intent. There is a need to raise awareness of both cultural differences and their possible impact.

Awareness

Electronic commerce and electronic authentication are still emerging disciplines. The level of awareness of both the technologies and their use is patchy and in many cases fraught with misconceptions. This is particularly the case in respect of the security and reliability of the technologies and their implementation. There is a need to raise awareness among government policy makers, business managers and individual users. In many cases it will be difficult to focus attention on just electronic authentication as a large proportion of the target audience will have wider ranging responsibilities or interests. Strategies for raising awareness of electronic authentication technologies and associated issues will often need to be integrated with broader electronic commerce awareness raising strategies. Specific electronic authentication awareness raising programmes can be developed and targeted at selected audiences.

Leadership

Governments, international organisations, business, users and user groups and the IT industry all have to assume leadership roles if electronic commerce in general and electronic authentication in particular are to flourish. Adoption of clear legal and policy frameworks, standards and business practices as well as use of the technologies themselves will provide the leadership required to ensure the widespread uptake of electronic commerce.

Conclusion

It was not the objective of the Task Group to make specific recommendations in this paper. Rather the paper has been prepared to identify relevant issues for APEC member economies and the various working groups of APEC that will need to consider the issues and develop options in consultation with the wider international community.

APEC TELECOMMUNICATIONS WORKING GROUP
BUSINESS FACILITATION STEERING GROUP
ELECTRONIC AUTHENTICATION TASK GROUP

ISSUES RELATING TO THE USE OF ELECTRONIC AUTHENTICATION

What is a Digital Signature ?

It is the means by which the recipient of a transaction or message can make an assessment as to whether to accept or reject that transaction.[94]

INTRODUCTION

The opening quotation was part of a task group report specifically addressing issues relating to digital signatures. However, as the role of the task group has widened to address all types of electronic authentication, so can the question be expanded. The quotation is equally relevant to all types of electronic authentication.

For the purposes of both the Electronic Authentication Task Group and this paper, the term 'electronic authentication' covers the authentication of individual and organisational identity, roles and attributes. Electronic authentication schemes and technologies may also cover message integrity and non-repudiation in addition to authentication. As part of the technology neutral approach, the following terms are used throughout the paper, with or without the prefix 'electronic':

- Authenticator -- a parameter for the authentication of individual or organisational identity, roles or attributes.
- Authentication technology -- the technology used to generate, issue or interpret an authenticator.
- Authentication service provider -- a body that generates, issues, receives or stores all or part of an authenticator and might add some further service (for example a certification authority in public key cryptography terms or the holder of a biometric template);

---

94. Asia Pacific Economic Cooperation, Telecommunications Working Group, Business Facilitation Steering Group, *Public Key Authentication Task Group Preliminary Report,* September 1997, http://www.apecsec.org.sg/telewg/16tel/bfsg/matrix/TELEWG-BFSG-3e-2.html

- Authentication scheme -- a scheme that involves authenticators and authentication service providers.

- Certificate -- an electronic document generally issued by a third party that binds an authenticator to a specified user.

- Cross certification -- the practice of cross recognition of another authentication service provider's authenticator to an agreed level of confidence and is normally evidenced in a contract or agreement. (An extension of the concept used in public key infrastructures).

- High-level authentication authority -- a body with responsibilities relating to the activities of a number of subordinate authentication service providers (For example a root authority in a public key infrastructure or a government licensing body).

It was also recognised that a number of economies are federations with a number of state or provincial governments that, in some cases may have legal jurisdiction over all or part of commerce. For that reason the term jurisdiction has been used rather than economy.

A number of alternative approaches are identified, and in some cases detailed, throughout this document. These are only put forward as possible solutions and the Electronic Authentication Task Force does not recommend that member economies adopt these particular approaches. In some cases they will form the basis for further discussion within APEC.

BACKGROUND

Electronic commerce transactions including financial, human resources, registrations, online shopping and document exchanges, are invoked through a number of online applications such as e-mail, Web browsers and EDI. As the transition from a paper-based legal framework to electronic means continues there is an increased urgency to ensure that these transactions are secure and, where appropriate, legally binding and auditable.

Authentication schemes provide the authenticity and, in some cases, integrity of transactions. As governments and private institutions continue to expand their electronic networks to serve the public directly and conduct business with organisations external to their own, the requirement to certify and establish a level of trust between the organisations becomes more important.

At the 15th meeting of the Asia Pacific Economic Co-operation (APEC) Telecommunications Working Group (TEL) in March 1997, it was agreed to establish a task group to review and assemble information about international trends in public administration with respect to public key authentication. The Task Group presented its preliminary report to TEL 16 in September 1997.

In September 1998, a workshop on public key authentication and a meeting of the APEC Public Key Authentication Task Group were held in conjunction with APEC TEL 18 in Port Moresby, Papua New Guinea. As a result it was agreed that the Task Group (renamed the Electronic Authentication Task Group) develop an awareness raising paper expanding on a number of issues identified as being critical to the implementation of electronic authentication. The paper would also need to identify any unique needs,

either in business models or electronic authentication requirements, in APEC member economies and focus on ensuring cross border recognition of electronic authentication techniques within the APEC region.

The Task Group and Workshop identified the following issues to be addressed in this paper:

- Definitions.
- Business models.
- User requirements.
- Technology.
- Trust.
- Liability.
- Roles of participants.
- Interoperability.
- Accreditation.
- Cultural differences.
- Awareness.
- Leadership.

The Task Group agreed to the preparation of a technology neutral report addressing the main issues relating to the use of electronic authentication. It also agreed to the production of four technology specific annexes addressing the following groupings of technologies:

- Asymmetric cryptography.
- Shared secrets.
- Biometrics.
- Other.

A further two annexes were subsequently requested:

- Hybrid technologies.
- An explanation of cryptography.

The annexes will cover how the specific technologies address the issues raised in the main body of the report.

It further agreed that the main report and the annex relating to asymmetric cryptography would be presented to TEL 19 and the three remaining annexes to TEL 20.

DEFINITIONS

The first problem encountered in examining this subject was the question of definitions and terminology. As electronic commerce has evolved certain terms have become synonymous with specific technologies. For example the term digital signatures is generally related to the use of public key cryptography and the term electronic signature is now used to cover other electronic signing processes. Similar problems emerge where a term has different meanings depending on where it is used. The problem became apparent in the preparation of this paper as the term ‘certification’ had one meaning in respect of public key infrastructures and another in respect of standards accreditation processes.

In addition as noted in an Organisation for Economic Co-operation and Development (OECD) paper[95] prepared for the 1998 OECD Ministerial Conference in Ottawa, certain terms have come to be used in very specific ways in technical communities but are often used inconsistently in policy discussions. The OECD is continuing to address this issue.

The International Organization for Standardization and the International Electrotechnical Commission Joint Technical Committee on Information Technology, Sub Committee 1, Vocabulary (ISO/IEC JTC1 SC1) has the formal task of standardising the vocabulary for information technology.

In many cases a term can have a different meaning depending on its context. It is therefore unlikely that complete consistency can be achieved. There is a role for member economies to contribute to and stimulate both the OECD and ISO work in attempting to achieve the maximum degree of consistency. However, member economies also have a role in encouraging the inclusion of definitions in particular documents. Governments can play a leadership role by adopting this practice for their documents.

ELECTRONIC BUSINESS MODELS

Electronic business models can be categorised on the basis of the environment in which they operate. There are several definitions under discussion in various communities to categorise certification authorities by business model and this work can be extended to describe business models in general. Some of these definitions are discussed below:

Open Model

An open model involves the use of electronic authenticators between users who do not have a pre-arranged or organisational relationship covering reliance on the particular authenticator. It assumes there are many parties who may rely on an authenticator but who may not have been known to each other at the time of issuance of the authenticator.

Typical of open models would be where a user enters into a business contract with a third party based on the exchange of electronic authenticators validated where necessary by reference to a service offered by an authentication service provider. In this case the parties are independent legal entities although there may be a legal relationship between one of the parties and the authentication service provider.

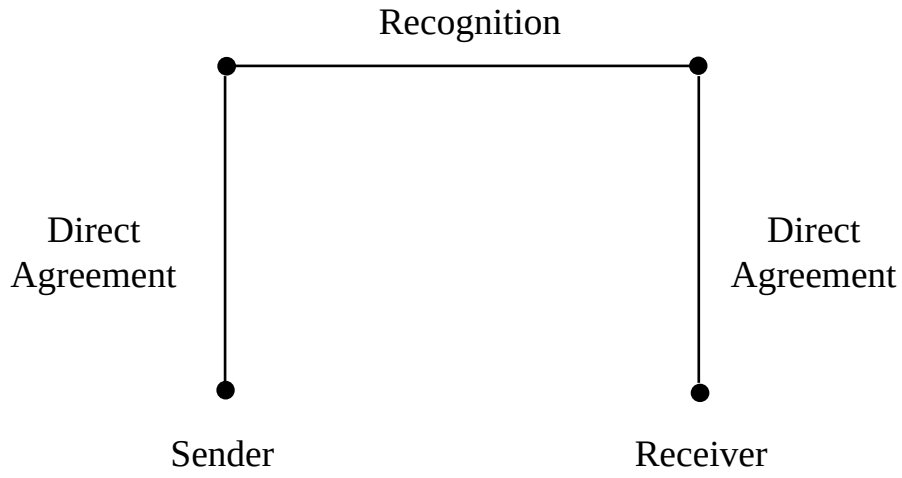
The classic example of an open model is Internet business where two parties may enter into a transaction without any prior contact or formal arrangement.

The main advantage of this model is that it allows a business an almost unlimited field of potential clients. However in many cases establishment of a business relationship goes beyond simply authentication of identity and other aspects such as financial viability, ability to deliver goods etc are often established and taken into consideration. These could reduce the ‘openness’ in many cases.

---

95. Organisation for Economic Cooperation and Development, *Inventory of Approaches to Authentication and Certification in a Global Networked Society*, Paris, October 1998, http://www.oecd.org/dsti/sti/it/ec/prod/reg_3e.pdf

Figure 1 - Open Model



Source: APEC.

A Closed Model

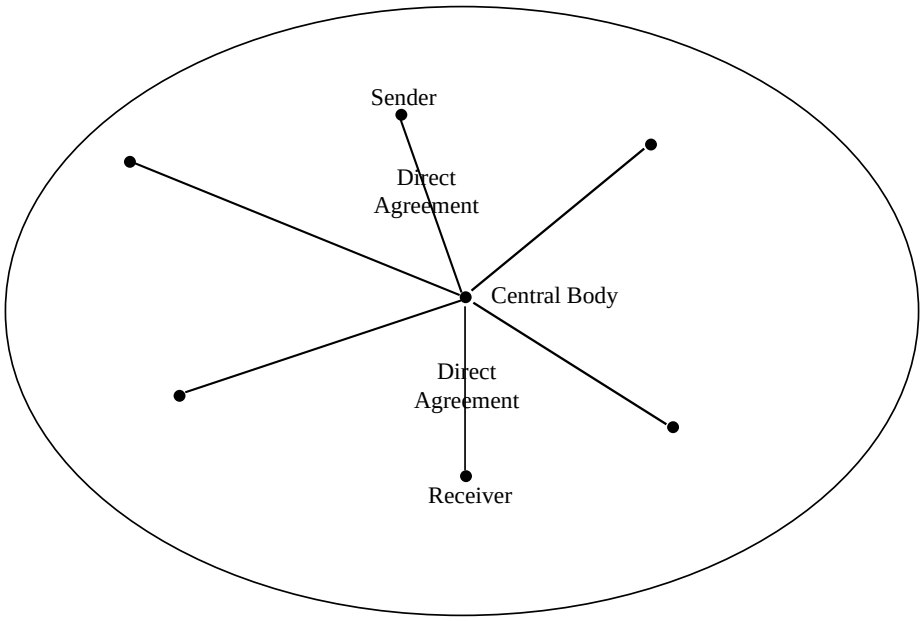
A closed model is one in which authenticators are exchanged between users who have a pre-arranged contractual or organisational relationship which extends to the issue and use of authenticators.

Typical of closed models would be authenticators exchanged internally between employees of a corporation or government (organisational relationship) or authenticators exchanged between users and a hub organisation such as between a business and its customers or suppliers where an agreement on the use of authenticators exists (contractual relationship).

Examples of closed models would be value-added networks such as EDI where formal agreements exist; or online merchants who request that a client establish an account. A number of banks have also established closed systems for dealing with their customers.

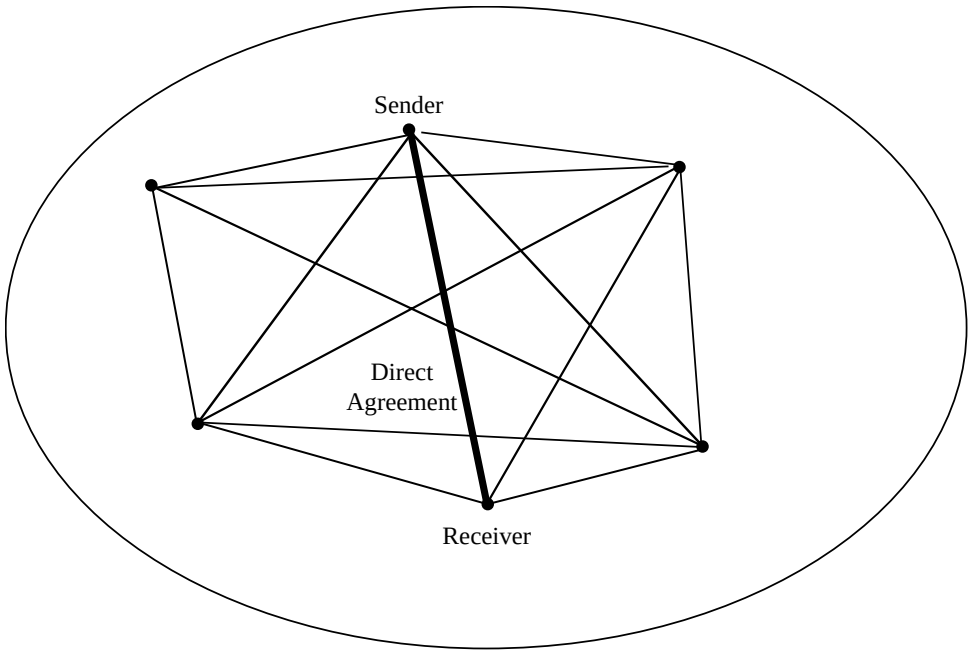
The main advantages of this model are that the business can retain its relationship with its client and the greater certainty in dealing within established relationships.

Figure 2(a) - Closed Model Example 1



Source: APEC.

Figure 2(b) - Closed Model Example 2



Source: APEC.

Open-but-bounded model

There is a third model sometimes referred to as open-but-bounded. In this model multiple parties could rely upon an authenticator but limits would be placed on the possible number of relying parties and trust would be gained through advance agreement by known parties.

Typical of open but bounded models would be where a number of relying parties agree to accept an authenticator issued by one or more specified authentication service providers.

An example of an open-but-bounded model would be one where a government decides that its clients can use a single authenticator issued by any one of a number of authentication service providers. The authenticator be recognised by a number of agencies without there being formal agreements in place. This is the model adopted by the Australian Government in its Project Gatekeeper.[96]

A draft paper by Michael Baum of Verisign observes[97]:

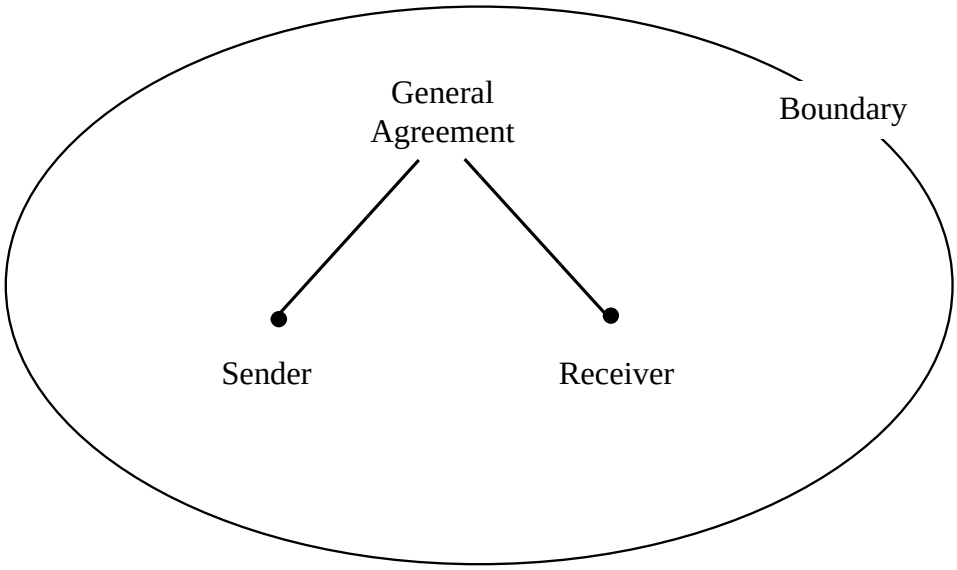
'A closer look at "open" PKIs in actual commercial practice demonstrates a very different reality. Open PKIs often become constrained, or bounded, just prior to use by relying parties.'

The example quoted is somewhat different to that outlined above. However, there is growing recognition that open models may be bounded in some way.

96. Office of Government Information Technology, *Government Online GATEKEEPER A strategy for public keytechnology use in the government*; http://www.ogit.gov.au/gatekeeper/pub/GATEKEEPER.pdf

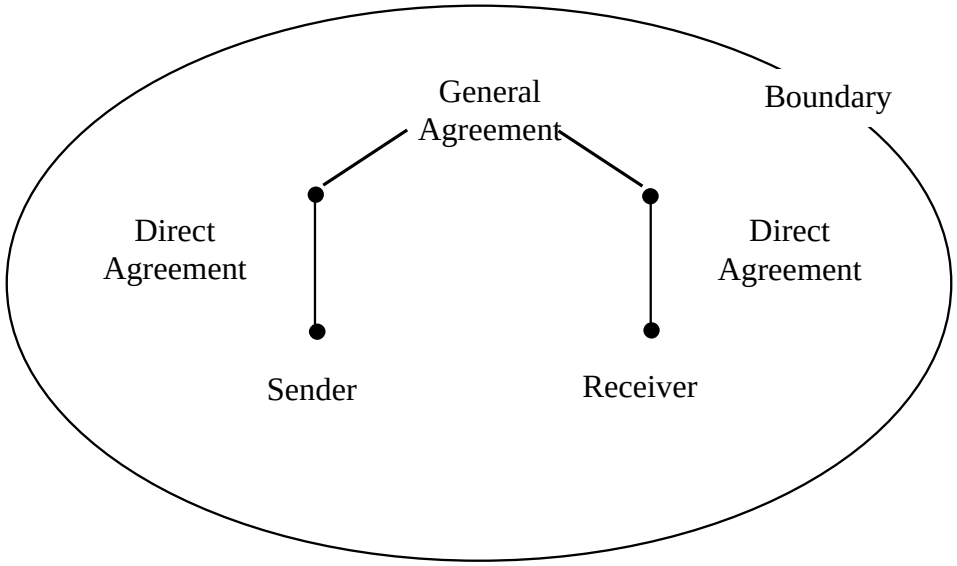
97. Michael S. Baum, Technology Neutrality and Secure Electronic Commerce: Rule Making in the Age of "Equivalence", http://www.verisign.com/repository/pubs/tech_neutral/

Figure 3(a) - Open-But-Bounded Model Example 1



Source: APEC.

Figure 3(b) - Open-But-Bounded Model Example 2



Source: APEC.

One problem that is becoming apparent, irrespective of the business model, is that in the move to electronic transactions, a number of implementers are assuming that some form of electronic authentication is required. In some cases electronic authentication is being used in transactions where signatures are not used in the equivalent paper process. This can place electronic transactions at a disadvantage, in terms of cost and bandwidth associated with the authenticator and in public acceptance of electronic transactions.

While business process re-engineering is an important element in the development of electronic commerce, it is important to ensure that some of these processes do not, inadvertently, place greater demands on and or costs to businesses and users.

USER REQUIREMENTS

Most users of electronic commerce do not and will not understand the complexities of the security and authentication services that they require in order to conduct business safely over telecommunications infrastructures.

The one thing that they do realise is that they need confidence in the system that they are using and confidence in the surrounding infrastructure. Further users also need relatively simple and foolproof methods of engaging the security and authentication services that they require.

The following is a list of user requirements that has been formulated by the World Electronic Messaging Association (WEMA). This is a grouping of the individual Messaging Associations from around the world.

(a) Encryption -- it shall be possible to send encrypted messages and attachments though any/multiple service providers.

(b) Encryption algorithms -- the messaging system shall be capable of en(de)crypting messages using different algorithms and the algorithm shall be transparent to the user.

(c) En-route encryption options - there shall be different options for en-route encryption: end-to-end (User Agent to User Agent), Link (Message Transfer Agent to Message Transfer Agent) and, Network (local user Message Transfer Agent to remote user Message Transfer Agent).

(d) Authentication - there shall be bi-directional recognition of authentication. The sender shall be able to authenticate the recipient and the recipient the sender.

(e) Repudiation -- proof of delivery shall be such that a receiver cannot deny having received a message. Likewise the same sort of proof shall be available such that the sender cannot deny having sent the message.

(f) Encryption key lengths - there shall be no restriction on encryption key lengths.

(g) Confidentiality -- users shall be able to specify that a message is confidential and the service provider shall ensure that the message is encrypted in such a fashion that no access to the message can be made while it is in transport.

(h) Traffic patterns -- service providers shall not observe user traffic patterns and therefore shall not be able to deduce abnormal activity levels (*e.g.* increased traffic prior to a merger or acquisition).

(i) Virus detection -- mechanisms shall be provided to protect against and detect viruses contained in message attachments. If a virus is detected the originator and recipient shall be warned.

(j) Mandatory routing -- there may be times when it is desirable that a message does not transit through certain countries, or transit through certain service providers. There shall be a mechanism for a user to specify a mandatory route.

The WEMA group is also working towards making the above requirements a reality.

The above list was prepared by one business group. Other Business groups are working on defining their own requirements. This gives rise to two potential conflicts. The first is that inconsistencies will develop between perceived needs of the various business groups. The second is that governments will introduce policies and legislation that do not adequately meet the user needs. The need for continued dialogue between the different interests is obvious.

Technical requirements

More specifically than those items mentioned above, security procedures and authentication should be as transparent as possible for users. A user should be able to readily verify an authenticator incorporated in a message or transaction. Unless this procedure is simple or transparent, most users will not bother.

Business process requirements

Users will need to be educated in the procedures required to verify information in the electronic world. There needs to be discussion on why and when security procedures are required.

It is incumbent upon business entities such as the Chambers of Commerce and the accounting bodies to ensure consistency in the procedures for the electronic environment just as we have built up paper based procedures

Legal requirements

Users need to feel confident that any transactions or messages acted upon which have used correct security procedures will be backed up within the legal environment. The APEC Legal Issues survey[98] covers these issues very well.

Government endorsement

Governments need to back the establishment of a global electronic community in which the citizens of each economy can feel as if they have all of the rights and responsibilities that they are accustomed to in the normal paper based environment.

98. Asia Pacific Economic Cooperation, *E-Com Legal Guide*, http://www.apii.or.kr/telwg/e-com/index.html

ELECTRONIC AUTHENTICATION TECHNOLOGIES

In examining authentication technologies, the Task Group identified four grouping as follows:

- Asymmetric cryptography.
- Shared secrets.
- Biometrics.
- Other.

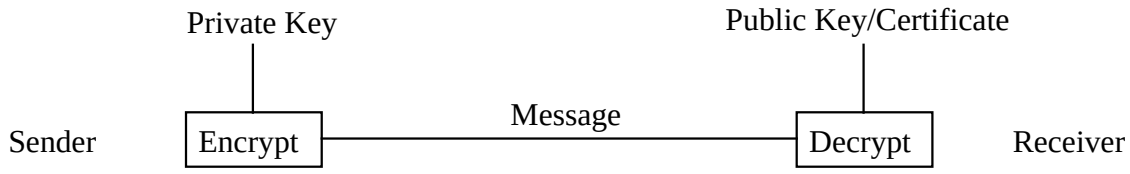
In addition the Task Group noted there was a trend towards using a combination of several authentication technologies for several transactions. The name 'hybrid' was attached to this group.

Asymmetric cryptography

This group covers public key cryptography which many people see as synonymous with electronic authentication. It is also known as digital signature technology. Technologies in this group provide functions of authentication, integrity, non-repudiation and confidentiality. Asymmetric cryptography can be used to authenticate identities and attributes and can be used in open, closed or open but-bounded environments. It can also be used as a tool to ensure the integrity documents without using the authentication capability. Again this can occur in open, closed or open-but-bounded environments. An important element is the existence of public and secret components (known as keys) and for access to the secret component to be controlled by the owner. One of the policy issues is the question of control over secret, or private keys, particularly in respect of key generation which is discussed in the Annex A. This technology is the only one that provides a message integrity capability.

While the concept and some technical implementations are very mature, it is only in recent years that the infrastructures required to support widescale deployment of this technology have started to emerge.

Figure 4 - Asymmetric Cryptography



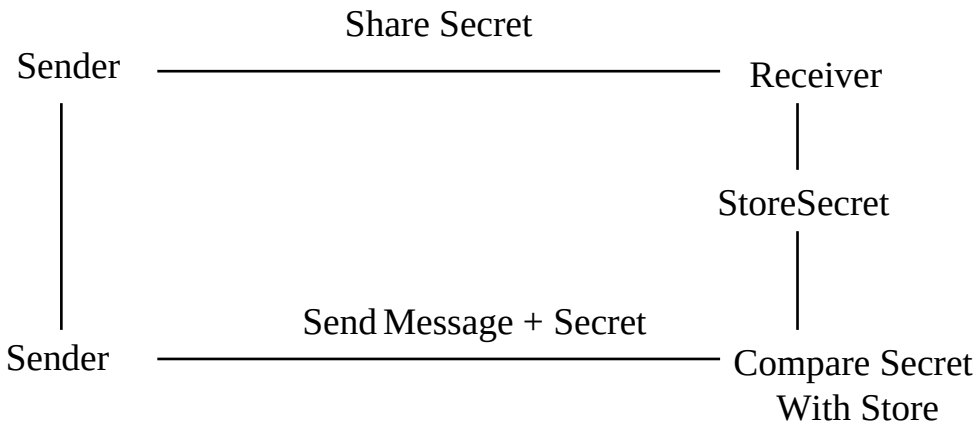
Source: APEC.

Shared secrets

This group covers implementations such as symmetric cryptography; passwords/PINS; and challenge/response. Technologies in this group provide for authentication. However, only symmetric cryptography can provide confidentiality and integrity capabilities in some implementations. Depending on whether the secret is unique to each pair of parties, non-repudiation is possible. This group mainly supports closed business models as the secret has to be shared between both parties and there is likely to be some form of associated arrangement. It can, however, support open-but-bounded models through a chaining arrangement where an authenticator in one closed system could generate an authenticator for another closed system. For example Kerberos could be used in this way.

A number of the technologies in this group have been in use for many years. Some businesses have indicated a preference for operating on shared secret technologies at this stage as they are more familiar with the associated business risks.

Figure 5 - Shared Secret



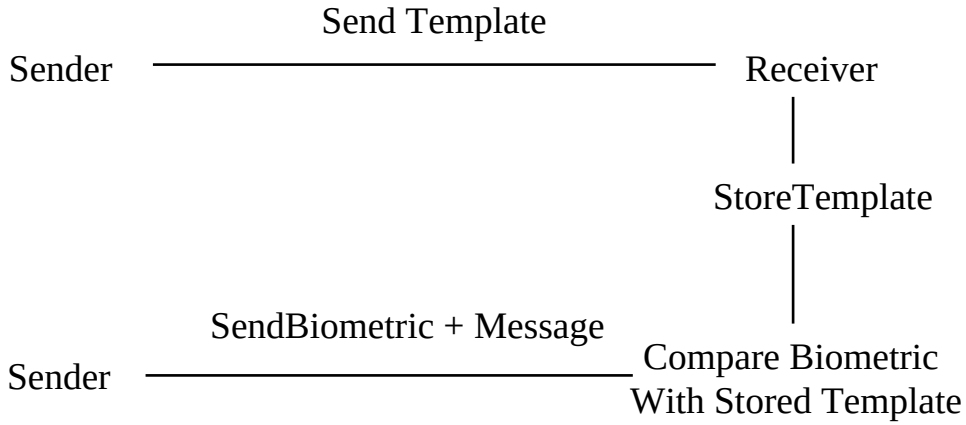
Source: APEC.

Biometrics

This group covers a range of technologies that use personal characteristics as an authentication techniques. It includes fingerprints, hand geometry, retina/iris patterns, signature/keyboard dynamics and voice verification. Other characteristics may be used in the future. Technologies in this group provide for authentication and non-repudiation. Biometrics rely on the recipient being able to compare a biometric with some form of template or the original of the characteristic. However, it is possible for templates to be certified and stored for comparison in the same way as public keys are in asymmetric cryptography. This group could, therefore, support open, closed and open-but-bounded models.

Biometrics have been used for physical access control for many years. However these implementations were closed systems. Problems emerge in the protection of templates in the more open electronic environments. A number of implementations are using cryptographic techniques to protect templates and communication of biometric characteristics. For this reason many implementations of the technologies will fall under the hybrid heading.

Figure 6 - Biometrics



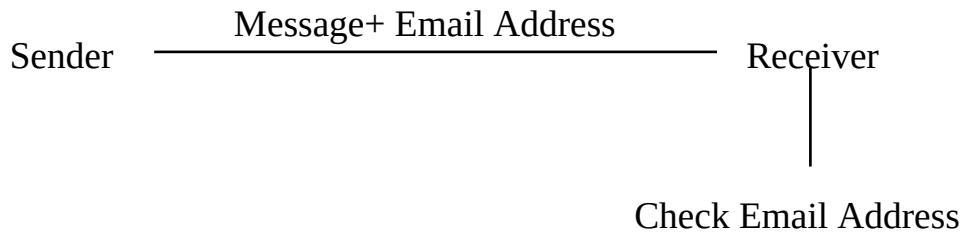
Source: APEC.

Other

This group covers a number of characteristics of a message or transaction rather than specific technologies. These include e-mail address, domain name, IP address, and the signature block on a message. This group only covers authentication but the technologies can be used in open, closed and open-but-bounded models.

Use of authenticators from this group is actually very widespread. It is one of the most common means of authentication currently used, particularly in respect of e-mail. Generally it is used in association with other collateral evidence such as expectation of the communication, shared knowledge of events or introduction by a third party. This results in an aggregation of trust. Its use for high risk/value transactions can be expected to diminish as the technologies discussed above become more widely available. It will, however, continue to play a part in both low value transactions and in closed systems such as organisational e-mail for the foreseeable future.

Figure 7 - Other E-mail Address Example



Source: APEC.

Hybrid

It is becoming apparent that in a number of instances several technologies are being utilised in a single transaction. PenOp uses signature dynamics for authentication combined with cryptography for message integrity. Passwords are passed over the Internet using cryptography (*e.g.* SSL in browsers) to protect them. Biometrics are being used to trigger a digital signature (asymmetric cryptography) which on receipt generates a Kerberos ticket (symmetric cryptography) to access a particular file. The question is at what point do you separate the authentication process from the associated security process. Ultimately that will be a matter for courts to decide and will probably vary from case to case. However the legal and policy frameworks for electronic authentication need to be flexible enough to cover these hybrid technology approaches.

Figure 8 - Hybrid Using Three Technologies

Source: APEC.

Selection

The selection of the appropriate electronic authentication technology is one of risk management and will vary over time as technologies in the different groups emerge and are superseded. Users will need to examine the assets they are trying to protect and the risk to those assets before selecting the most appropriate technical solution. Other issues would include cost/benefit and integration with other technologies. The decision is one for users and not for government. Legal and policy frameworks need to be flexible enough to allow users to make the choice of the most appropriate technology for their purpose. Governments may, however, have a role in ensuring that technologies and their implementations meet their stated objectives and that users are able to make informed choices. These issues are discussed elsewhere in this report.

CERTIFICATION MODELS

Several of the technologies outlined in the previous section require a third party to certify the identity of the holder of a particular electronic authenticator. As early as 1996[99] distinctions were being made between formal and informal certification approaches. For the purposes of this paper three basic certification approaches are considered.

---

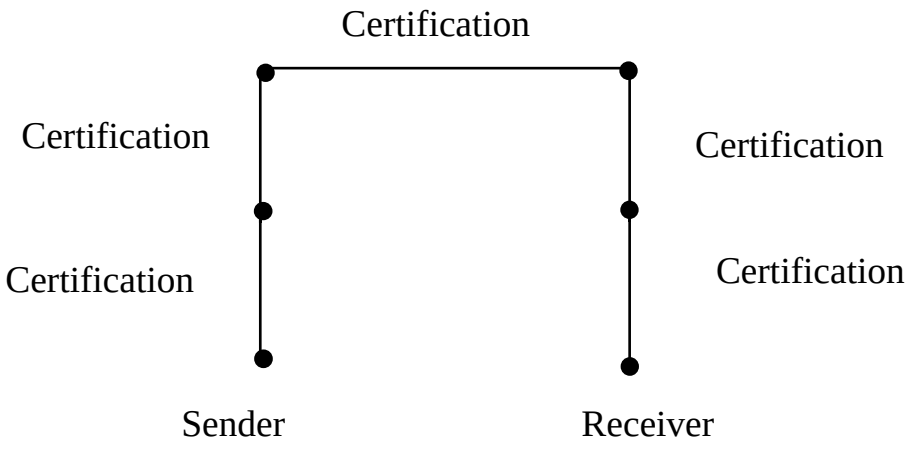
99. See for example abstract to paper *Let A Thousand (Ten Thousand?) CAs Reign* Stephen Kent, BBN Corporation, http://jya.com/dimacs.txt

Formal certification

This approach generally involves an authentication service provider formally taking on the role of binding a party to a particular electronic authenticator. A number of approaches involve hierarchical structures with each level being certified by a higher element until a peak is reached. For this reason it is also referred to as a chain of trust. These bodies may be established within an organisation or may be provided on a commercial basis. The Public Key Infrastructure (PKI) approach is an example of a formal certification approach. PKI approaches can range from small implementations within an organisation to elaborate hierarchical models that can cover millions of key holders. An IETF standard, Public-Key Infrastructure (X.509) (pkix), exists for this approach.

It is also possible for biometric templates to be bound to an individual party. This approach is not yet in common use and no standards are available.

Figure 9 - Formal Certification



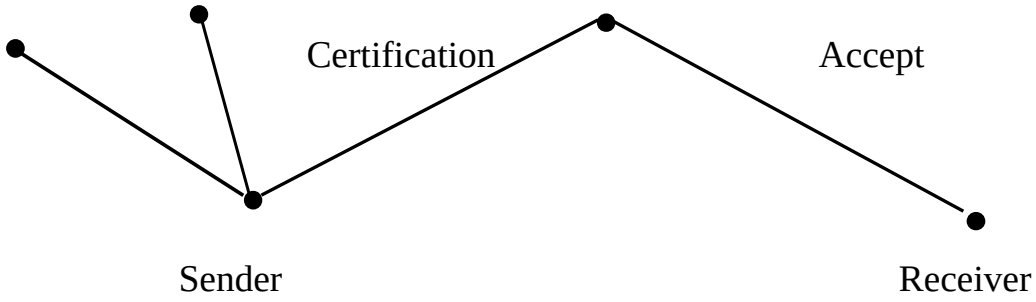
Source: APEC.

Informal certification

This approach generally involves a third party or a number of third parties certifying that an electronic authenticator belongs to a particular party. A relying party checks to see if it trusts one of the certifiers. This technique is used for public keys in approaches such as Simple Distributed Security Infrastructure (SDSI), Simple Public Key Infrastructure [SPKI] and in the PGP suite of products. It does not rely on the formal hierarchical structure that is common to formal certification and is often referred to as a web of trust. An IETF standard, Simple Public Key Infrastructure (spki), exists for this approach.

In theory it may be possible to informally certify biometric templates but no examples of such approaches could be found.

Figure 10 - Informal Certification



Source: APEC.

No certification

A number of electronic authentication technologies do not require, or can exist without, any form of certification. Shared secret implementations require the parties to know each other before the secret is shared. Therefore there is no need for certification where this technology is used.

The 'other' group of technologies does not lend itself to the use of either formal or informal certification although it may be argued that some of the 'introductory' aspects such as a party advising a third party's e-mail address does add some element of increased trust when dealing with the third party. As no 'certificate' is created or utilised, this approach has been included in the 'no certification' model.

Both asymmetric cryptography and biometrics can be used without certification.

Figure 11 - No Certification

Source: APEC.

TRUST

Much has been written about the need to develop user trust or confidence in the new technologies including electronic authentication[100]. This includes trust that the technology can deliver the benefits (economic, productivity) and trust that the user will not be disadvantaged by using it (fraud, privacy, consumer issues).

Trust can be achieved through the development of appropriate technology, development of appropriate legal and policy frameworks and development of appropriate business practices. In all cases not only do these elements need to be developed but users need to be aware of the developments and the issues involved.

Many of the sections of this report are ultimately directed at developing frameworks that will generate user trust. For example, accreditation processes are designed to enable users to trust the technologies while legal frameworks are designed to enable users to trust that they can rely on the legal validity of a transaction. Awareness raising programmes are designed to build the level of required trust once the appropriate frameworks are in place.

As these elements are discussed in more detail in this report the discussion will not be duplicated here.

LIABILITY

There are a number of liability issues that need to be addressed. These include:

(a) Liability of the user for misuse of their authenticator, including failure to adequately protect the key from misuse.

(b) Liability of an authentication service provider.

(c) Liability of users and authentication service providers during the revocation process.

(d) Liability of an authentication service provider for losses incurred through failure to provide a service or for negligence in providing a service.

There have been some suggestions that liability should be addressed through legislation. Others feel that contractual arrangements would suffice although there is a "contract privity problem" involved where the recipient has no prior contractual arrangement with either the user or the user's authentication service provider.

---

100. See for example: Asia Pacific Economic Cooperation, *APEC Economic Leaders Declaration: Connecting the APEC Community*,Vancouver, Canada, November 25, 1997 http://www.apecsec.org.sg/econlead/vancouver.html, Organisation for Economic Co-operation and Development, *Dismantling the barriers to global electronic commerce*, Paris, November 1997, http://www.oecd.org/dsti/sti/ec/prod/dismantl.htm

The "contract privity problem" has existed in aspects of international trade for centuries. While the scale of electronic commerce will increase dramatically with the uptake of the new technology, existing approaches to international trade may, in the short term, be able to handle problems that arise.

The OECD addressed these issues as they relate cryptographic authenticators in the Liability Principle of its Cryptography Policy Guidelines.

> "7. LIABILITY
>
> "WHETHER ESTABLISHED BY CONTRACT OR LEGISLATION, THE LIABILITY OF INDIVIDUALS AND ENTITIES THAT OFFER CRYPTOGRAPHIC SERVICES OR HOLD OR ACCESS CRYPTOGRAPHIC KEYS SHOULD BE CLEARLY STATED.
>
> "The liability of any individual or entity, including a government entity, that offers cryptographic services or holds or has access to cryptographic keys, should be made clear by contract or where appropriate by national legislation or international agreement. The liability of users for misuse of their own keys should also be made clear. A keyholder should not be held liable for providing cryptographic keys or plaintext of encrypted data in accordance with lawful access. The party that obtains lawful access should be liable for misuse of cryptographic keys or plaintext that it has obtained."

This principle could be extended to any authentication scheme in which case the thrust of the principle would be that contracts or legislation can be used to establish the liability of users or authentication service providers.

While liability can be clearly established between a user and his/her authentication service provider through the contact terms and conditions at the time an authenticator is issued or received, this does not assist the recipient in establishing liability if he or she relies on an authenticator. While it would be impractical to include all terms and conditions with an authenticator to allow the recipient to make a judgement, it may be possible to develop a series of model terms and conditions which could be referenced with the authenticator.

There is also the question of whether governments should limit liability to encourage the establishment of authentication service providers. The counter argument is that limiting liability may discourage electronic transactions of a value above the legislated liability limit. In these cases it may be necessary to allow users, recipients and authentication service providers to negotiate a contract incorporating liability greater than the statutory limit possibly based on a higher fee. Limiting liability may also discourage rigorous adoption of standards by authentication service providers and detract from the trust and certainty sought to be achieved by authentication schemes.

Decisions as to whether to adopt contractual or legislative approach will be a matter for individual jurisdictions. However, when considering which approach to adopt, jurisdictions need to take into consideration that other jurisdictions may take the other approach and make appropriate provisions for accommodating the differences.

ROLES OF PARTICIPANTS

The Community of Interest applicable to electronic authentication includes:

- Governments.
- High-level authentication authorities (optional).
- Authentication service providers.
- Users.

The term 'users' includes end-entities/users/subscribers depending on the terminology used in a particular architecture. They may be independent or associated with a sponsor recognised by an authentication service provider. A sponsor is an organisation with which an end-entity/subscriber/user is affiliated (*e.g.* employee of a firm).

The term 'Relying Party' is used in some system documentation to define the recipient of an authenticator who acts in reliance on that authenticator. By that definition authentication service providers and users are all relying parties during specific processes and exchanges in a PKI supported system.

All elements of the community of interest have roles particularly in respect of ensuring the integrity of the authentication scheme or schemes.

Governments

It is the role of government to provide the legal, regulatory and policy frameworks to support electronic authentication. The balance of legal and self-regulatory approaches will vary from jurisdiction to jurisdiction. In some implementations, the activities listed below may be performed by government in which case it would need to take on the additional roles.

High level authentication authorities

In some cases or for some authentication technologies it may be decided to establish one or more high-level authentication authorities. These may be established by government, industry groups or even individual organisations managing one or more authentication service provider. In some cases high level authentication authorities may be involved in the accreditation or licensing of their subsidiary authentication service providers.

Roles of high-level authentication authorities could include:

(a) Providing or approving policy and practice statements for subsidiary authentication service providers.

(b) Ensuring compliance with applicable legal provisions, policy and practice statements, technical standards.

(c) Facilitating cross-certification as discussed in the next section.

Authentication service providers

It is the role of authentication service providers to:

(a) Advise users of the authentication service provider's policy and practice statements.

(b) Make copies of documented cross-certification agreements including relevant policy and practice statements available to subscribers of all certified and cross-certified authentication service providers.

(c) Revoke authenticators and publish revocation lists as required under the relevant policy statement.

(d) Perform the identification and authentication procedures stipulated in the applicable policy statement.

(e) Provide authentication and repository services consistent with the policy statement.

(f) Provide the operational, security and technical controls stipulated in the policy and practice statements.

(g) Comply with all applicable policy and legal provisions.

(h) Accept liability for elements of damage and financial loss arising from or in connection with its services as warranted in the relevant policy statement or in accordance with relevant laws and regulations.

Users

Users have roles in ensuring that:

(a) No unauthorised party has had access to any secret component of an authenticator.

(b) All representations made to an authentication service provider in the course of obtaining an authenticator were true.

INTEROPERABILITY

The issue of interoperability means different things to different people. It has been argued in some quarters that we should be aiming for a single globally interoperable scheme. Others support the concept of a number of globally interoperable schemes. As mentioned earlier different technologies will meet different requirements based on risk, cost and integration with other technologies. It is unlikely that the differing requirements can be met by a single scheme without compromising risk at one end or cost at the other. However too many schemes will confuse users, possibly increase costs as users need to implement an excessive number of schemes and leave users with a bewildering array of technologies attached to their systems. The objective should be to minimise the burden on users in order to encourage them to adopt

electronic authentication and electronic commerce. Government and industry need to pursue an appropriate balance in consultation.

Interoperability covers technical interoperability, cross border recognition of legal and policy frameworks and, more specifically, cross-certification within authentication schemes.

A number of these issues were canvassed in the Task Groups preliminary report and are included here in an updated form.

Technical standards

International technical standards will be essential for ensuring interoperability of electronic authentication. A number of national and international standards bodies are addressing these issues. There is the potential for the development of inconsistent standards in these different arenas. In addition, a number of industry sectors are also developing their own systems or products based on proprietary or industry group standards. Clearly there is the potential for short-term problems of interoperability with the various approaches. To be too dogmatic about particular standards, however, has the potential to stifle developments in both the authentication technology and the interoperability processes.

The standards exercise needs to be examined at two levels; detailed standards for particular technologies and their use, and standards for interoperability between the different technologies. The former can, to a certain extent, be developed in isolation although it is important that interoperability be considered even at that level. The latter must be developed at a full international level. Even regional approaches have the potential for inconsistencies which can cause problems for inter-region interoperability. If this emerges as a significant problem, APEC member economies may need to take a pro-active role in international standards making bodies to ensure full interoperability is achieved.

A number of APEC economies are active in the international standards arena and can assist in progressing these issues in those forums.

Cross border recognition of legal and policy frameworks

Some see the ideal situation as having consistent legislation across all jurisdictions. However, inconsistencies are already starting to emerge in legislative approaches in different jurisdictions. This problem may be exacerbated in some federal structures where state or provincial governments may adopt legislative approaches inconsistent both between each other and with that of the federal government. In some cases these inconsistencies can be quite significant, for example mandatory use of particular authentication technologies or government licensing of authentication service providers versus a completely free market approach. Other problems arise from legislation containing detailed specifications of the technology and procedures that need to be adopted.

Another difficulty which arises is that, whilst particular legislation might be seen to be highly desirable and may be strongly advocated by the technical or business sectors, such proposed legislation might in practice be unlawful or unenforceable when reviewed against the legal rights provisions of the constitutions of, or the common laws in, other member economies. It is likely that some fundamental legal rights provisions are in fact included in all civil and common law jurisdictions and any proposals to introduce procedures

which are not consistent with such fundamental legal rights, however desirable they may be from the technical or business viewpoint, are doomed to failure.

The United Nations Commission on International Trade Law (UNCITRAL) has developed a Model Law on Electronic Commerce [101]and is undertaking work on rules for electronic signatures. Any significant APEC work in this area would be an unnecessary duplication of the work being carried out by UNCITRAL.

A number of APEC economies are active in the UNCITRAL arena and can assist in progressing these issues in that forum.

As highlighted in a number of areas throughout this report, the biggest danger to the interoperability of electronic authentication schemes is overly specific legislation or regulation. Schemes that mandate particular approaches to the exclusion of all others, be they technical, legal or procedural, will not be able to accept authenticators from schemes that do not adopt the same approach. However, schemes that adopt more flexible approaches will be able to accept authenticators from schemes that mandate approaches. This will disadvantage schemes that adopt the mandatory approach in terms of electronic commerce. From the broader perspective, it will establish barriers to international interoperability.

In some cases it may be possible to introduce schemes of a particular model for internal use within an economy. The problems emerge when the scheme mandates that particular type of scheme for all transactions regardless of where they originate. This can be overcome by technology neutral legislation which does not specify that a particular approach must be used for transactions to be acceptable.

While this somewhat oversimplifies the problem, there will be a need for governments to consider how to achieve national objectives in some of these areas without formulating legislation which would have the effect of precluding schemes which operate on a different basis.

In its preliminary report, the Task Group recommended that further work be carried out with other international organisations. In general, these are cases where positive guidance has to be given in addressing a problem, rather than avoiding specifying particular approaches. In most cases, this further work needs to be carried out in conjunction with other international bodies. This can be approached in a number of ways:

(a) The establishment of a formal liaison mechanism between the Secretariats of the various organisations.

(b) Exchange of official observers for relevant meetings.

(c) Exchange of draft documents between members of various groups.

(d) Nominating representatives already members of the other bodies to act as liaison points.

(e) Conduct of joint meetings, seminars etc.

---

101. United Nations Commission on International Trade Law, *Model Law on Electronic Commerce*, New York, June 1996, http://www.un.org.at/uncitral/texts/electcom/index.htm

In fact a combination of these approaches may be the most appropriate. The important thing is to establish a dialogue with these other bodies to ensure that work is not duplicated, or worse, develops in different directions.

Cross-certification

There is a requirement to establish a consistent and auditable level of trust between authentication schemes. A formal method of certification known as "cross-certification" is being developed[102]. The scheme is being developed for public key infrastructures but the same principles can be used for other authentication service providers that use the same basic authentication technology (*e.g.* biometrics).

The process of cross-certification includes reciprocal legal, technical and policy review of authentication scheme policies and authentication scheme practice statements, their implementation and operational management. This is to ensure that the authentication service provider of each respective domain agrees and meets the standards as set out in its authentication scheme policy and authentication scheme practice statement and that these are essentially equivalent. If there is agreement on their equivalence, a formal process leading to a mutual agreement in the form of a contract allows the authentication service providers to cross certify with each other. The process must allow for changes and co-ordinate these in a timely fashion to prevent interference with organisational programmes and business transactions. Cross-certification agreements should have a fixed term and allow for renewal, termination and amendments.

Cross-certification can take place at a single or multiple levels of assurance. Programmed site inspection of the cross-certified authentication service provider facilities must occur in order to ensure the integrity of the agreements.

A further issue that is starting to emerge is interoperability between authentication technologies and other technologies used in the process of generating, transmitting or receiving a transaction. We are already starting to see instances where authentication technologies can be rendered ineffective by other technologies. For example firewalls and gateways can reject digital signatures or encrypted measures as they could possibly be maleficent code or contain viruses. There is a need to encourage co-operation between product developers and implementers to ensure that unnecessary barriers are not erected.

ACCREDITATION

One of the main issues to be addressed is whether government should license or regulate authentication technology or authentication service providers. A number of possible scenarios emerge:

(a) Government licensing.

(b) Government endorsed accreditation scheme.

---

102. See for example: Electronic Commerce Promotion Council of Japan, Certification Authority Working Group, *Publication of "Exposition of Cross-Certification Technology and Proposed Basic Specification"*, http://ecom.ecom.or.jp/eng/output/97report_summary/wg08-2.htm, United Nations Commission on International Trade Law, "planning of future work on electronic commerce: digital signatures, certification authorities and related legal issues", http://www.un.or.at/uncitral/english/sessions/wg_ec/wp71.htm

(c) Standards based accreditation scheme.

(d) Industry endorsed accreditation scheme.

Implementation of these schemes can be mandatory or voluntary. The type of approach adopted will vary from jurisdiction to jurisdiction determined largely by domestic policy on issues such as industry regulation and consumer protection. Problems will emerge if jurisdictions insist that authentication technologies or service providers satisfy their licensing or accreditation processes and requirements even where the service provider or user of the technology is located outside their immediate jurisdiction.

As mentioned at the outset, the key requirement of authentication schemes is to allow the recipient of a message or transaction to make an assessment as to whether to accept that transaction. To be able to make that judgement, the recipient needs to be aware of the type of accreditation the authentication scheme or technology has received as well as any relevant cross-certification information. The means by which accreditation and cross-certification information is conveyed to a recipient needs to be standardised.

Authentication service providers accreditation process

In both mandatory or voluntary schemes, the chain of confidence in authentication services can be established on a sound footing by developing an effective accreditation and certification system. This system relies on independent judgement being made at each level of the system. In the first instance, the certification bodies make a judgement as to whether the service provider's operations (*i.e.* authentication services) complies with a relevant standard. The certification body is judged to be competent to carry out the relevant certification by an accredited body. The certification and accreditation process are both carried out by independent bodies. With such a process in place in two countries, the chain of confidence can then be completed by the accreditation bodies making judgement in the competence of each other's programmes.

The criteria against which the service of an applicant is assessed are those outlined in an international/national Standard or a normative document nominated by a regulatory body.

Depending on the development of standards and other normative documents internationally (or nationally) a service provider could apply for certification in one of the following methods:

(a) If there is an international/national standard available, the applicant can approach a national/international certification body to obtain certification in its authentication operations. The evaluation (and the certification) work is carried out by the certification body (or a subcontracted body on behalf of the certification body). Following satisfactory compliance of the relevant criteria/standard the service provider receives certification to operate within a defined infrastructure as a certified authentication service provider.

(b) If there are other normative documents available, the applicant can approach the relevant regulatory body for guidance on achieving certification in its authentication operations. The evaluation (and the certification) work is carried out by nominated evaluators on behalf of the regulatory body. Following satisfactory compliance of the relevant criteria/standard the service provider receives certification to operate within a defined infrastructure as a certified authentication service provider.

The following is a step by step guide to the accreditation process used in the standards environment:

(a) **Identify what goals are required to be achieved.** The typical objectives/goals in applying for certification will be to be more efficient and profitable, produce better services, achieve customer confidence and satisfaction, increase market share, improve communication within the service provider's organization and to reduce costs and liabilities. Identification of what the customers and end users, suppliers, shareholders, community and employees expect of the services will also be beneficial in assessing the need to apply for certification.

(b) **Service Provider registers with the appropriate Certification body.** The service provider should contact several certification bodies to find out what is offered, what the likely costs are, the period for which the certification will apply and how frequently they will want to audit the system. Some certification bodies may include an initial pre-assessment in their offer. This can be of major benefit in finding out the current status and what needs to be done. When the service provider registers with the Certification body, a project coordinator may be appointed by the Certification body for liaisons, and the relevant documentation detailing certification requirements will also be forwarded.

(c) **Service Provider prepares required documentation for certification.** The service provider should obtain information about the certification criteria and prepare all required documentation and apply the certification criteria to the authentication operations to ensure/demonstrate conformance.

(d) **Service Provider forwards relevant documentation to the Certification body for evaluation.** The Certification body may carry out the certification work themselves or subcontract this work to a recognised evaluator. It may be necessary for certification bodies (or evaluators) to make a number of site visits or reviews of documentation, dependent on the need for further evaluation. For example, a physical security review may recommend changes to locks, doors etc. The service provider will need to carry out any work recommended and be re-evaluated to ensure compliance.

(e) **The service provider obtains certification from the Certification body.** When all criteria has been reviewed to the satisfaction of the Certification body, a certificate of Certification will be presented to the service provider confirming that it may now advertise, market and operate as a certified service provider within a defined infrastructure. A list of certified service providers may also be published either by the accreditation or the certification body.

(f) **Certification maintenance.** The service provider will be required to maintain the certification by notifying the Certification body of any changes in its services and carrying out a periodic audit as required by the Certification body.

Authentication Technology Accreditation Process

While accreditation of specific authentication technologies is part of the process of accrediting an authentication service provider, it can also be applied to the technology alone. This would assist in generating user confidence in the products that they, rather than the service provider would be using.

The steps involved are similar to those set out in the section above but would be limited to the product itself.

CULTURAL DIFFERENCES

During the course of its workshop in Port Moresby, and subsequent discussions, the Task Group has become aware of a number of cultural differences within the APEC region that can affect the way electronic authentication is implemented. The first difference noted involves various concepts of community property rather than identifiable individual or joint ownership of property. The community property concept can cover extended families or clans, village or tribal groupings. Many electronic authentication techniques have as central themes the concepts of binding an electronic authenticator to an individual and for the authenticator to be under the control of that individual. It is difficult to translate electronic authentication techniques that rely on the concept of individuals to cultures whose basic concepts are communal. These community property concepts are present in a number of APEC member economies.

The second difference involved the signing process and the means by which agents sign on behalf of the principal. In a number of Asian member economies, chops are used rather than written signatures. A principal can assign an agent signing privileges by providing the chop. In economies where written signatures are used, agents are provided with a written power of attorney by the principal and the agent applies his or her own written signature on behalf of the principal. Similar processes apply in respect of delegated authorities. Again the electronic authentication concept of individual control over an authenticator does not translate to an environment where the cultural approach is the transfer of the signing instrument.

In both the above examples, legal frameworks may be based on the cultural concepts.

These are only examples of cultural differences and have been presented to highlight the need for governments to be sensitive to the existence of cultural differences between economies. These cultural differences have the potential to impact on technical, legal and policy aspects of electronic authentication. Often cultural differences are not addressed in these aspects through ignorance rather than intent. There is a need to raise awareness of both cultural differences and their possible impact.

AWARENESS

Electronic commerce and electronic authentication are still emerging disciplines. The level of awareness of both the technologies and their use is patchy and in many cases fraught with misconceptions. This is particularly the case in respect of the security and reliability of the technologies and their implementation. There is a need to raise awareness among government policy makers, business managers and individual users. In many cases it will be difficult to focus attention on just electronic authentication as a large proportion of the target audience will have wider ranging responsibilities or interests. Strategies for raising awareness of electronic authentication technologies and associated issues will often need to be integrated with broader electronic commerce awareness raising strategies. Specific electronic authentication awareness raising programmes can be developed and targeted at selected audiences.

Government awareness

Government policy makers shape the framework within which electronic authentication will operate. In doing so they need to be aware of the international as well as national environment in which the

technologies will be used. In most governments there are a large number of policy makers, very few of whom participate in international discussion of electronic authentication issues. This is particularly true in federal structures where the state or provincial governments are rarely directly involved in the international policy development process. There is a need to give all relevant government policy makers access to information on both national and international issues relating to electronic authentication. An awareness raising strategy could include newsletters, seminars and workshops and information resources.

Seminars and workshops need to be conducted at both the national and international level with the aim of meeting national objectives while ensuring cross border recognition of laws and policies. As mentioned earlier some of these activities need to address electronic commerce in general with electronic authentication as a component, while others need to be specifically designed to address electronic authentication issues in some detail. Part of the strategy would be to identify a high level champion to encourage attendance at these seminars and workshops.

In keeping with the electronic nature of the subject, electronic media can be used for awareness raising. There are already numerous electronic resources, newsletters and list servers dealing with electronic commerce and electronic authentication. The main problem is finding them. One project this Task Group has been asked to carry out is to establish a Website that provides links to resources on electronic authentication. This Website could be developed in co-operation with other international bodies.

Governments will not be able to carry out the leadership role or develop user confidence unless able to convince their constituents that they have the necessary awareness of the issues and have developed appropriate responses.

Business awareness

Governments have an interest in encouraging the uptake of electronic commerce to obtain the associated economic advantages. Industry bodies have an interest through their role of maximising the efficiency and profitability of their members. These outcomes can only be achieved if business recognises the advantages of the new technologies and has the confidence to use them.

To achieve these outcomes, there are a number of areas where business awareness needs to be raised. These include awareness of the role of electronic authentication in supporting the business advantages of electronic commerce, awareness of the available electronic authentication technologies and their implementation, and awareness of the government and industry group frameworks to support electronic authentication.

As mentioned earlier both governments and industry have an interest in promoting the new technologies. It would be appropriate for awareness raising strategies to be developed as a co-operative activity between the two. The establishment of government/industry co-ordination bodies to develop strategies for awareness raising is one step that can be implemented. The identification of champions within industry sectors to carry the message to their colleagues is another important element.

The small business seminars on electronic commerce conducted by Australia Oceania Electronic Messaging Association (AOEMA) in a number of economies under the auspices of APEC TEL are a good example of the type of business awareness raising programmes that can be implemented.

In addition to the information resources and seminars and workshop approaches discussed in the previous section, another awareness raising activity is pilot projects. Business may be more prepared to participate in a pilot activity than to commit to something in isolation. Experiences from a pilot would increase their

awareness and also that of their peers and clients and can contribute significantly to awareness raising on a sectoral or industry group basis. A number of pilots are being conducted in and between APEC economies and some are reported to APEC TEL. These reports can provide a valuable awareness raising resource.

As with government, awareness raising is part of the leadership role of business.

Individual user awareness

There is still considerable apprehension and misconception among individual users on the subject of both electronic commerce and electronic authentication. Much of this relates to the security of their transactions and payments. Unless this is overcome they will not utilise the new technologies.

While there are a number of focal points for government and business through which awareness raising campaigns can be directed, this is not the case for individuals. Any strategy for this group needs to have two elements. First there is a need to raise the awareness of and obtain support from key representative associations such as user groups, consumer groups etc. Second there is a need for broadcast campaigns through various media channels building, where appropriate, on any support from representative groups. Representative groups should be included in any awareness raising strategy group.

Word of mouth is still important in awareness raising; both in a positive and negative sense. An individual's experience in use of electronic authentication can influence the decisions of a number of associates. A negative impression will spread faster than a positive one. It is important for business to recognise that failures, even in pilot projects, have an awareness raising impact.

LEADERSHIP

The leadership required to encourage the practical usage of electronic authentication clearly will vary according to the circumstances in each economy. The following suggests some of the initiatives that may be appropriate. Broadly, leadership is required from:

- Governments.
- International organisations.
- Business corporations.
- Users and user groups.
- IT industry.

Governments

The first critical requirement is that governments should publish as early as possible their overall policies with regard to the establishment of authentication schemes. Such policies need not initially be too detailed, but their complete absence will seriously impede many related developments. The private sector, and indeed government departments, cannot make their own plans with any certainty and surely will be reluctant to invest scarce capital resources without the reasonable probability that their own authentication scheme will integrate smoothly into whatever it is that the government proposes.

Possible government policy models can be very different.

(a) Government may decide to leave the authentication arena wide open. Government may or may not establish one or more authentication schemes within its own departments and related organisations, the private sector being free to set up authentication schemes, commercial or otherwise, as it sees fit. There would be no high-level authentication authority and authentication service providers would be responsible for ensuring interoperability with other service providers, domestically and internationally, depending upon the objectives in establishing that authentication scheme. No licensing or technology approvals of authentication service providers would be required, save for the usual consumer protection regulations.

(b) Government may decide to establish either a voluntary or mandatory high-level authentication authority. In this case other authentication service providers may find it necessary to interoperate with the high level authentication authority if they wish to have their authenticator accepted outside their own systems. In this case, the technical and management specifications of the authentication service providers must be published as quickly as possible so that both government departments and the private sector may plan accordingly. Licensing and technology approvals for each authentication service provider could be required.

(c) Government may decide to establish one central and national authentication service provider to the exclusion of any others within the economy, except perhaps for some special purpose authentication service providers established with government approval.

International organisations

Appropriate international organisations try to monitor developments in various economies and should regularly issue policy advice papers to all governments, setting out the advantages and disadvantages of adopting particular policies, based on actual successes and failures.

Such international organisations need to play a co-ordinating role to assist economies to establish authentication schemes under their control to inter-operate with authentication schemes that are not under their control.

Some international bodies are standards bodies, and where required they should reach an early consensus on authentication standards and publish them as soon as possible.

Business corporations

Business corporations, being major users of authentication schemes, have a particular responsibility to adopt schemes that are compatible, where appropriate, with the authentication schemes being adopted internationally.

In particular, such business corporations should not seek to impose their authentication schemes on their trading partners, unless such schemes are compatible with the internationally accepted schemes.

Users and user groups

Individual users and their representative groups have a role to play in encouraging the uptake of electronic commerce and electronic authentication. Personal recommendations by individual users carry significant weight. These views can be built on by user groups who can make appropriate recommendations. However, any adverse experiences and associated publicity can have a devastating effect on development.

Governments and industry need to work with users and user groups to ensure that proposals meet user requirements and users will take an appropriate leadership role in encouraging user uptake.

IT industry

The IT industry, especially the developers of authentication schemes, must strive towards, and take active steps to try to achieve, international interoperability.

It should be a guiding development principle that if a developer introduces an authentication technology that is, of itself, not interoperable with internationally accepted schemes, then that developer should ensure that his product is equipped with effective gateways to ensure international interoperability. It should not be necessary for the user of an internationally accepted authentication scheme to have to modify his international scheme in order to accommodate the non-international scheme.

Conclusion

It was not the objective of the Task Group to make specific recommendations in this paper. Rather the paper has been prepared to identify relevant issues for APEC member economies and the various working groups of APEC that will need to consider the issues and develop options in consultation with the wider international community.

EESSI

AN INDUSTRY INITIATIVE IN SUPPORT OF THE EUROPEAN DIRECTIVE ON ELECTRONIC SIGNATURE

Claude Boulle, Groupe Bull - Hans Nilsson, Id2 Technologies

Background

The development and use of authentication products and services is still in its introductory stage. Systems exist which use authentication for commerce, administration and public services, however, there is no complete set of agreed industry standards or technical specifications for their use. Without such standards it is not considered possible to provide a common level of security which can be recognised as being valid for use at regional level, *a fortiori* at international level.

The Communication of the European Commission "A European Initiative in Electronic Commerce" identified the need for electronic signatures as a key issue for electronic commerce. Whilst the signing of contractual exchanges for electronic commerce are not the sole application of electronic signatures it is likely to become an essential component for the future of European business in the competitive global market.

On the request of the Council, the European Commission has proposed a Directive to provide a common framework for electronic signatures. It is not the intent of this Directive to cover the whole domain of applications of authentication, but rather to focus on the legal validity of an electronic signature attached to an electronic document with the same legal effect attached to an handwritten signature on a paper document. However, contractual freedom should prevail for "electronic signatures used within closed groups, for example, where contractual relationships already exist". The Directive identifies minimal requirements for trusted service providers supporting electronic signatures as well as requirements for signers and verifiers. These requirements need to be underpinned by detailed standards and open specifications which can be recognised as meeting these requirements so that products and services supporting electronic signatures can be known to provide legally valid signatures.

Several standardisation initiatives have already been launched at the national, regional and international levels by organisations and industry fora. Worth mentioning are the activities of the International Chamber of Commerce, the UNCITRAL activity on Model Law, the ILPF current inventory, the IETF and ABA standardisation activities. They are however, at this stage, not necessarily sufficient to respond to the legal requirements. A consistent and coherent approach is necessary, so that the legal framework for electronic signatures can build, as far as possible, upon standards and other forms of voluntary agreements which can be used to provide signatures which can be recognised as legally valid not only across Europe, but at international level.

In order to provide timely standards permitting full and efficient implementation of a common framework, based on consistent Member States' legislation, standardisation initiatives should be encouraged at an early stage, in particular so as to obtain adequate international co-operation.

The mandate from the Commission

Industry and European standardisation bodies, within the frame of the ICTSB, have been requested by the European Commission to analyse in a coherent manner, the future needs for standardisation activities in support of essential minimum legal requirements, as stated in the Directive in relation to electronic signatures products and services to be made available to the market. The assessment of available standards and current initiatives at global and regional level, both in formal standardisation bodies and industry consortia, should identify gaps and the need for any additional standardisation initiatives in all relevant forms, such as standards, specifications, agreements, workshops or any other form of consensus building. On the basis of this analysis, an indicative work programme should be proposed.

It is thus for Industry and European Standardisation bodies to set up the implementation framework, compliant with the minimal legal framework stated by the Directive, which will answer business needs and bring the full advantage of the legal recognition of the electronic signature in support of the development of the open electronic commerce environment.

The establishment of EESSI

To meet the requirements of the Commission mandate, the ICTSB has launched the European Electronic Signature Standardisation Initiative (EESSI) placed under the direction of a steering group composed of:

- Industry representatives, members of organisations such as HLSG (High Level Strategy Group for ICT Standardisation) and EEMA.
- ICTSB member organisation representatives with an interest.
- Representatives of the European Commission.
- Industry experts.

The Steering Group is assisted in its work by an Expert Team with the following members:

Hans Nilsson, ID2 Technologies, Sweden (Project leader)
Patrick Van Eecke, Univ Louvain, Belgium (Legal Expert)
Manuel Medina, Univ of Catalunya, Spain
Denis Pinkas, Bull, France
Nick Pope, Security & Standards Consultancy, UK

In addition, a “Review” Team has been appointed consisting of:

Leslie Seymour, consultant
Bart Preneel, Univ Louvain, Belgium
Bob Willmott, consultant, UK

The task of the Expert Team

The expert team will produce a report as the starting point for the steering group to meet the EESSI objectives, *i.e.* to prepare the grounds for the necessary standardisation activities and the identification of the standardisation needs in support of the emerging legal framework for electronic signatures in the European Union, based on an assessment of existing standards and technical specifications in this area.

The legal requirements set by the proposed Directive focus on certificates and certification services to ensure minimum levels of security and to allow their free movement throughout the Single market. Standardisation efforts should therefore be oriented towards establishing transparent, proportionate and non-discriminatory rules for such certification schemes.

In addition to certificates and certification services covered by the scope of the proposed Directive, standardisation activities could also cover the off-line use of electronic signatures and electronic signature products and services to be made available to the end-user.

Requirements have to be considered in an open environment, in close co-operation with all relevant parties; subsequently adequate and efficient co-operation mechanisms should be put in place in view of establishing international-wide consensus among all parties concerned. Arrangements will therefore also be proposed to establish the relevant international co-operation to ensure that the relevant standards are available at global level.

Preliminary findings

The expert team has been very active during the last few months, and has also had many contacts with other experts and organisations, both in Europe and internationally. The report will be presented in an Open Forum meeting in Brussels on 1st July 1999. It will be available by mid-June for consultation at the following address :

http://www.ict.etsi.org/eessi/EESSI.htm

The preliminary findings of the expert team indicate needs for standardisation in the following areas:

- Specification of a first set of services and mechanisms needed to support electronic signatures, based on digital signature technology.
- Profiles for the usage of existing PKI standards, such as those developed by the IETF PKIX group.
- Specification of security management for service providers supporting electronic signatures.
- Certificate policy for qualified certificates used to create advanced electronic signatures.
- Security requirements for protection of private keys supporting electronic signatures.
- Specification of requirements for signature creation and verification of products.
- Syntax and encoding of electronic signatures and signed documents.

ILPF – SURVEY OF INTERNATIONAL ELECTRONIC AND DIGITAL SIGNATURE INITIATIVES

Project Overview

The Internet Law & Policy Forum commissioned Steptoe & Johnson LLP to survey current legislative and regulatory efforts outside the United States concerning digital and electronic signatures.[103] This report provides a comparison and analysis of electronic authentication initiatives in jurisdictions outside the United States, including international efforts at the United Nations Commission on International Trade Law (UNCITRAL), the Organisation for Economic Co-operation and Development (OECD), and the European Union (EU).

This report complements, and in many respects builds on, the ILPF Survey of Electronic and Digital Signature Legislative Initiatives in the United States (the "ILPF US Survey"). The report assumes familiarity with digital signatures and electronic authentication generally; readers desiring more background should refer to the "Background" and "Authentication Models" sections of the ILPF U.S. Survey. For ease of reference, this report summarizes the legislative initiatives described herein in the same table format as the ILPF U.S. Survey.

ILPF and the authors seek public comment on this report, and welcome additional information and corrections concerning the initiatives discussed in this report. We particularly encourage readers to submit information about new legislative and regulatory initiatives that are not discussed in this report, as we intend to update the report on a regular basis. Any comments should be sent to the ILPF, intsurvey@ilpf.org. and to the authors, Stewart Baker and Matthew Yeo.

Introduction: Overview of legislative initiatives

Perhaps the most significant observation about legislative initiatives outside the United States is how few of them there have been to date. This report identifies only six countries that have enacted legislation

103. This report will adopt the reasonably well-established distinction between "digital signatures," *i.e.*, the process of authenticating an electronic record with an asymmetric cryptosystem using the signer's private key, and the broader category of "electronic authentication" techniques that may include digital signatures, biometrics, signature analysis, or other methods. This latter category is sometimes referred to as "electronic signatures."

specifically relating to electronic authentication: Argentina, Germany, Italy, Malaysia, Russia, and Singapore.[104] By contrast, according to the ILPF US Survey, 36 states have introduced or are considering legislation concerning electronic signatures, with 26 states having enacted some type of legislation. In fact, a number of other U.S. states have since passed legislation relating to electronic authentication, so these numbers are now higher.

As in the United States, however, there have been a large number of official studies and proposed legislative initiatives that have not yet come to fruition. Australia, Austria, Belgium, Colombia, Denmark, Hong Kong, China, South African Republic, Korea, and the United Kingdom are in the process of reviewing and adopting proposed legislation. Canada, Finland, France, Ireland, Japan, the Netherlands, and New Zealand have published reports, consultative papers or policy statements on electronic authentication issues, and other countries are in the process of preparing similar reports.[105]

It is difficult to compare national approaches to electronic authentication legislation because so few countries have conceived of the purpose of such legislation in quite the same way. Some countries, like Germany and Japan have, to date, focused only on the technical standards for the operation of a Public Key Infrastructure ("PKI"). Others, like Singapore and Malaysia, have spanned the entire range of issues associated with the legal effect of electronic signatures, the legal framework for the operation of a PKI, and the establishment of a regulatory apparatus to oversee Certificate Authorities ("CAs"). Indeed, one of the themes of this survey is that countries do not always agree on the required scope of electronic authentication legislation.

As discussed later in this report, several international initiatives are underway to harmonize national approaches to electronic authentication. These initiatives include the draft EU Directive on electronic authentication, the work of the UNCITRAL Experts Group in preparing Uniform Rules on electronic authentication, and a proposed international convention on electronic authentication. Thus, it appears increasingly likely that many of the issues discussed in this report will be addressed at the international level, perhaps even before they are taken up by national legislators.

---

104. The Russian legislation, adopted in 1995, contains only minimal provisions concerning digital signatures. The relevant portion of the legislation states: "The legal force of a document stored, processed and transmitted by means of automated and telecommunications systems may be confirmed by an electronic digital signature. The legal force of the electronic signature shall be recognised where the automated information system contains technical programme means making it possible to identify the signature in the regime established for the use thereof. ... The right to certify the identity of the electronic digital signature shall be exercised under license. The rules for the issue of licenses shall be determined by [Russian Federation] legislation." "See Russian Federation Information Act, No. 24-FZ", adopted by the State Duma on January 25, 1995. (Available in the Westlaw RUSLEGISLINE database, 1995 WL 139853). So far as the authors were able to determine, there have been no subsequent developments in Russia concerning electronic authentication.

105. It is important to note that a number of countries have adopted legislation or launched initiatives that relate solely to the use of electronic signatures in the public sector. The Argentine legislation relates solely to the use of digital signatures in the "National Public Sector," which generally includes the government and state-owned companies. Canada has established the "Government of Canada Public Key Infrastructure" for use of digital signatures in government business, and Australia has recently created a similar entity known as "Gatekeeper." While these and other public-sector initiatives are of interest, this report focuses primarily on legislation that affects the commercial use of electronic authentication techniques.

I. Legislative models

A. The tension between technological neutrality and legal specificity

Any legislative approach to electronic authentication must accommodate the inherent tension between the goal of technological neutrality and the goal of prescribing specific legal consequences for the use of electronic authentication systems. To the extent that legislation seeks to enable the use of diverse electronic authentication techniques, including some that are not yet even conceived, it becomes progressively more difficult to accord specific and meaningful legal consequences to their use. The reason for this inverse relationship is fairly straightforward : legislators' confidence in the security and reliability of known electronic authentication mechanisms allows them to grant greater legal benefits and presumptions to the use of those techniques. They may be less willing to grant the same level of legal benefits to as yet unknown techniques or to technologies that bear no imprimatur beyond recognition and acceptance in the marketplace.

This conundrum is the inevitable consequence of legislating against a backdrop of rapid technological change. As recently as 1995, when legislative initiatives began to emerge in the United States, the use of asymmetric, or "public key," cryptography as a means of creating "digital signatures" was widely perceived as the nearly-universal foundation for all electronic authentication. Indeed, it is safe to say that this perception continued well into 1997, both in the United States and abroad, and remains influential today. More recently, however, there has been growing recognition that other means of electronic authentication, including biometrics and dynamic signature analysis, will take on equal or greater importance in the years ahead.[106] In fact, some of these techniques -- and particularly those that are based on biometric features -- may prove to be more reliable and less susceptible to compromise than digital signatures.

In all likelihood, no single technology will prevail as the sole means of electronic authentication. Different technologies will likely be used in different settings and for different purposes. This diversity of authentication techniques, while generally promoting the expansion of electronic commerce, nonetheless poses a significant challenge for legislators, because not all technologies necessarily require the same legal infrastructure or may be accorded the same presumption of security and integrity. Many believe that the widespread use of digital signatures, for example, requires a legally established "trust infrastructure," or PKI, that defines the rights and obligations of the parties to an authenticated transaction, including the potential liability of CAs to third parties. Other technologies, such as voice authentication, may not require the same type of legally-defined trust infrastructure, although it is very hard to predict how any of these

---

106. Indeed, in the past year, there have been a significant number of announcements concerning the commercial availability of biometric authentication technologies. Some online merchants are already using voice recognition and fingerprints, for example, as a means of authentication. See, *e.g.* Rob Fixmer, "Tiny New Chip Could Pit Protection of Property Against Right of Privacy," *The New York Times*, September 28, 1998. In January 1999, the Intel Corporation announced that its new microprocessor, the Pentium III, would have the ability to transmit a unique serial number over computer networks, including the Internet. While this serial number authenticates a processor -- not a person -- it will nonetheless facilitate online authentication. Thus, it appears that there are several different directions in which authentication technologies are headed.

technologies will be used in widespread commercial practice and what their specific legal requirements will be.[107]

For those legislators and policy makers who believe that the continued expansion of electronic commerce requires a known and reliable authentication mechanism with established legal consequences, the preference is usually to enact legislation that specifically addresses the use of digital signatures, and to save the issues raised by other authentication techniques for another day. At the same time, legislators and policy makers naturally fear that any attempt to codify a known authentication mechanism -- namely, digital signatures -- runs the risk of stunting the development of other authentication mechanisms, or at least of giving undue benefits to a technology that is itself only in the earliest stages of commercial use. Apart from these concerns and the general desire to avoid the rapid obsolescence of new legislation, there is also a concern among national legislators and policy makers that premature endorsement of a particular technology will set the country outside of the mainstream of technological and legislative developments internationally.[108] For these reasons, "technological neutrality" in electronic authentication legislation has become an increasingly prevalent objective.

A typology of electronic authentication legislation

The manner in which legislators and policy makers have sought to accommodate the conflicting concerns described above largely defines the typology of existing and proposed electronic authentication legislation. While this typology encompasses many of the issues discussed in more detail below -- the legal effect of electronic signatures, licensing provisions, liability issues. -- it is nonetheless helpful to have a sense of the general approaches that national legislatures have taken.

1. The "Prescriptive" approach

To date, the most common approach has been to ignore authentication mechanisms other than those based on digital signatures, and to adopt what the ILPF Survey of US legislation refers to as the "prescriptive" approach. Argentina, Germany, Italy, and Malaysia have all enacted legislation that pertains solely to the use of digital signatures within a PKI, and the "Guidelines" issued by Japan's Electronic Commerce Promotion Council (ECOM) are similarly limited to digital signatures.[109] Significantly, these legislative

---

107. It seems likely, however, that even biometric techniques will require some sort of trust infrastructure -- as with cryptographic keys, some trusted third party must confirm the relationship between a particular biometric feature and a particular person or attribute of a person. Thus, it may very well turn out to be the case that the legal issues raised by the operation of a trust infrastructure are fairly generic to all authentication technologies.

108. As the recent Australian report observed, "Australia needs to be aware of international trends and developments in relation to electronic signature legislation before considering an appropriate regulatory framework for electronic commerce. Since the use of these authentication methods will relate to both domestic and international transactions, without this awareness Australia could find itself creating an unnecessary impediment to electronic commerce by the introduction of commercially restrictive or unworkable legislation or legislation which adopts a radically different approach to that taken in other jurisdictions."

109. Because of the brevity of the Russian legislation, it is unclear whether Russia falls into this category.

initiatives are among the oldest ("old" being a relative term, relating mostly to developments prior to early 1998), and, with the exception of Singapore, are also the only countries that have enacted legislation. More recent initiatives, whether in the form of proposed legislation or reports by national expert groups, have increasingly focused on the need to accommodate emerging and even unforeseen technologies.[110]

2. The "Two-Tier" approach

The second approach is what might be called the "two-tier" approach to electronic authentication legislation, referred to as the "hybrid" approach in the ILPF Survey of US legislation. At the first level, the legislation accepts all or most electronic authentication mechanisms on a technologically-neutral basis, and grants these mechanisms a basic set of legal benefits. For example, technologies that are accepted at the first level might satisfy writing and form requirements, but would not be entitled to any presumptions concerning the signer's identity or intent. At the second level, the legislation creates a class of approved technologies whose use is invested with a broader array of legal benefits and obligations. The legislation may define these technologies -- sometimes referred to as "secure" or "qualified" technologies -- by reference to general criteria, by reference to the specific techniques of asymmetric cryptography, or by reference to a schedule of technologies approved by statute or regulation. Documents that are authenticated by one of these methods are typically entitled to a more robust set of legal entitlements, for example, a presumption concerning the identity of the signer and the integrity of the document's contents. At this second level, the legislation may also seek to address issues that are specifically associated with the operation of a PKI, such as the operational requirements and liabilities of CAs.

The virtues of the "two-tier" approach are fairly self-evident. It achieves the goal of technological neutrality by granting a minimum level of legal recognition to all or most authentication techniques, mostly with regard to satisfying form and writing requirements. At the same time, it affords greater legal certainty and benefits to those authentication mechanisms whose security and reliability permit greater confidence in their use. This approach also recognizes that some authentication mechanisms, and particularly those that are used in open systems, require a better-defined legal environment (for example, because of the third-party liability issues associated with the use of digital certificates), while not depriving legal recognition to those authentication mechanisms that do not require a significant external legal framework (for example, because the parties establish the terms of their use by contract -- so-called "closed" systems).

Singapore's Electronic Transactions Bill, enacted in June 1998, is a good illustration of the two-tier approach. The ETB draws a basic distinction between electronic records and signatures, on the one hand, and secure electronic records and signatures on the other. An "electronic signature" is any set of letters, numbers, or other symbols in digital form attached to, or logically associated with, an electronic record,

---

110. As a recent report by the French *Conseil d'Etat* observed, "Il est sans doute préférable de s'en tenir dans le code civil à la reconnaissance des effets d'une signature électronique fiable authentifiant un message électronique, sans aborder les modalités du procédé de certification. Le parti inverse, retenu par l'Allemagne dans sa récente loi ..résente l'inconvénient majeur de faire peser un risque d'obsolescence sur le dispositif légal, compte tenu de l'evolution rapide des techniques." See *Internet et les réseaux numériques* (July 2, 1998), available at www.internet.gouv.fr. Similarly, in January 1999, the Australian government released a draft Electronic Transactions Bill and an accompanying explanatory report, which noted that "There appears to be an international trend away from legislation that prescribes the use of, or gives legislative advantages to specific types of signature methods such as digital signatures. … It is more appropriate for the market to assess appropriate signature products than have legislation specifying acceptable technologies."

and executed or adopted with the intention of authenticating or approving the electronic record. An electronic signature satisfies the requirement of a signature (with limited exceptions relating to wills, conveyances, and similar documents), and may be proved "in any manner." A "secure electronic signature," by contrast, is either a digital signature that comports with the ETB's digital signature standards or a "commercially reasonable security procedure agreed to by the parties." A secure electronic signature must be (1) unique to the person using it; (2) capable of identifying the person; (3) created through a means that is under the sole control of the person using it; and (4) linked to the electronic record in such a way as to confirm the integrity of the document. Documents that are authenticated by a secure electronic signature are entitled to a presumption of integrity, a presumption that the signature is that of the person with whom it is associated, and a presumption that the user affixed the signature with the intent of signing or approving the document. The ETB treats digital signatures as a type of secure electronic signature, and establishes a comprehensive regime for their use and regulation.

The draft EU Directive also illustrates the two-tier approach, although in a somewhat different manner.[111] The essential distinction drawn in the draft Directive is between "electronic signatures" and "qualified certificates." An electronic signature is one that satisfies the four criteria described above with respect to the Singapore ETB (uniqueness, identity, security, and integrity). The Directive would prohibit Member States from denying legal effect to an electronic signature solely on the grounds that it is in electronic form. A "qualified certificate," by contrast, is a "digital attestation which links a signature verification device to a person, confirms the identity of that person," and that satisfies the technical requirements specified in Annex I of the Directive (mostly pertaining to the contents of a qualified certificate). Member States would be obligated to ensure that electronic signatures based on qualified certificates satisfy the legal requirement of a handwritten signature and are admissible as evidence in legal proceedings in the same manner as handwritten signatures, but only if the electronic signature was generated using a "secure signature creation device" (as defined in Annex III of the Directive).

At the international level, the UNCITRAL Working Group on Electronic Commerce has also adopted the two-tier approach in the most recent draft of the Uniform Rules on Electronic Signatures. The draft Uniform Rules distinguish between "electronic signatures," which are those that satisfy the relatively broad requirements of Article 7 of the UNCITRAL Model Law on Electronic Commerce, and a narrower category of signatures (provisionally called "enhanced" electronic signatures) that satisfy a higher standard or that are executed according to the terms of an agreement between the parties.[112] Electronic signatures would satisfy any requirement for a signature "if the electronic signature is as reliable as appropriate for the purpose for which the electronic signature was used, in light of all the circumstances, including any

---

111. It is important to note that, as of February 1999, the EU Member States and the European Commission were actively negotiating the terms of the EU Electronic Signatures Directive. It is by no means certain whether these negotiations will succeed and, if they do, what the final provisions of the Directive will be. Thus, while our discussion of the EU Directive in this paper is based on the most recently available information, the draft Directive is not final and could change as negotiations proceed.

112. The standards for an "enhanced" electronic signature under the UNCITRAL Uniform Rules are provisionally the same as the Singapore ETB, namely, that the signature (1) is unique to the signer; (2) can be used to identify the signer; (3) was created using a means under the sole control of the signer; and (4) is linked to the data message in such a way that any change in the data message after signing would be revealed. The Working Group is continuing its consideration of this matter, however, and this definition is by no means settled. It is also important to note that the UNCITRAL Working Group is currently considering an alternative approach to the Uniform Rules, based on a significantly shorter draft that would limit itself to issues related to electronic signatures. The most recent draft of this shorter approach, UN Doc. A/CN.9/WG.IV/WP.80 ("WP.80"), would retain the distinction between electronic signatures and enhanced electronic signatures.

relevant agreement." "Enhanced" electronic signatures, on the other hand, would be entitled to a presumption that the data message was signed, a presumption that it was signed by the person associated with the signature, and a presumption that the data message was unaltered.

3. The "Minimalist" approach

Interestingly, several of the most recent national initiatives relating to electronic authentication have decided to forego any effort to legislate detailed standards for the use of different authentication techniques, and have taken a purely minimalist approach to granting legal recognition to electronic signatures. The March 1998 report of the Australian Electronic Commerce Expert Group, entitled Electronic Commerce: Building the Legal Framework, surveys a wide range of national and international approaches to electronic authentication legislation, and concludes that:

> … [T]he enactment of legislation which creates a detailed legislative regime for electronic signatures needs to be considered with caution. There is a risk, particularly given the lack of any internationally uniform legislative approach, that an inappropriate legislative regime may be adopted without regard to market-oriented solutions. Given the pace of technological development and change in this area, it is more appropriate for the market to determine issues other than legal effect, such as the levels of security and reliability required for electronic signatures. Accordingly, we have recommended that legislation should deal simply with the legal effect of electronic signatures.

The report further concludes that adoption of Article 7 of the UNCITRAL Model Law on Electronic Commerce, which creates broad standards for the recognition of an electronic signature, is the only legislative initiative required to create a framework for the use of different electronic authentication techniques. In this manner, the report specifically rejects the proposition that the widespread use of digital signatures and other electronic authentication methods requires a legal framework that allocates the rights, duties, and liabilities of the different parties to a secure electronic transaction.[113]

The recommendation of the Australian Electronic Commerce Expert Group was adopted in the draft Electronic Transactions Bill released by the Attorney General in January 1999. Article 10 of the draft Bill would give broad effect to electronic signatures where the method used to create the signature "was as reliable as was appropriate for the purposes for which the information was communicated."

II. Effects & Presumptions

Legal Effect

The most elemental objective of any electronic authentication legislation is to ensure that electronic signatures are accorded appropriate legal recognition. Virtually every jurisdiction has laws that require

---

113. A report recently issued by the New Zealand Law Commission appears inclined to take the same approach, although seeks comment on whether legislation should play any further role in facilitating electronic authentication.

that certain types of documents be "signed," or "in writing," or any one of countless other formulations that could be construed to require a physical document or handwritten signature. A report by the Canadian Department of Justice, for example, observed that the word "writing" appears 1 600 times in Canadian statutes, and other national surveys have produced similar results.

In attempting to resolve the issues surrounding the legal effect of electronic signatures and authenticated electronic documents, many countries have been influenced by Article 7 of the UNCITRAL Model Law on Electronic Commerce. Article 7 states that the requirements of a signature are satisfied with respect to a data message if (1) the method is used to identify the signer and to indicate that person's approval of the information contained in the message; and (2) the method is as reliable as was appropriate for the purpose for which the message was generated or communicated, in light of all the circumstances, including any relevant agreement between the parties. The means by which a particular jurisdiction will implement this standard, however, is likely to vary considerably according to the nature of its existing legal framework.

At least in common law jurisdictions, there is nothing about an "electronic signature" that is significantly different from a signature conveyed by a telegram, a telex, a facsimile, or by any of the other means that have been generally accepted in commercial practice and that are ordinarily accepted by most common law courts.[114] Nonetheless, whether as a result of specific evidentiary problems or out of a general concern that courts will be reluctant to accept electronic signatures, several jurisdictions have chosen to clarify the legal validity of electronic signatures. Providing such clarification is also seen as an important reassurance to parties that might otherwise be reluctant to use electronic signatures in commercial transactions. As noted above, Australia and its constituent states intend to adopt some variant of Article 7 of the UNCITRAL Model Law, and New Zealand is also likely to base its legislation on Article 7.

The situation in civil law jurisdictions tends to be somewhat more complex, given the civil law's generally more prescriptive approach to methods of proof and authentication. A recent report by the *French Conseil d'Etat* reviewed the various circumstances under the *Code Civil* where a handwritten signature or original document is required, as well as the hierarchy of evidence that the law requires for proving the validity of a signature (ranging, depending upon the circumstances, from a notarized signature all the way down to a faxed or photocopied signature). The report concludes that the *Code Civil* does not readily accommodate electronic signatures, and must therefore be amended to recognize, under most circumstances, the functional equivalence of certain "trustworthy" (fiable) electronic signatures.[115] Italy has already taken this step by establishing that digital signatures and electronic documents authenticated by a digital signature satisfy any form requirements and are accorded the same evidential weight as handwritten documents and signatures. In contrast to the French proposal, however, the Italian legislation only extends this benefit to digital signatures that are authenticated by licensed CAs.

Under the proposed EU Directive, Member States will be obligated to "ensure that an electronic signature is not denied legal effect, validity and enforceability solely on the grounds that the signature is in electronic

---

114. There are, of course, numerous situations in the common law where a traditional hand-written signature is required. The Statute of Frauds, for example, typically requires a contract for the sale of land to be in writing and executed with a hand-written signature in order for it to be enforced.

115. The French report states that "cette fiabilité est conditionnée par le respect des exigences suivantes: (1) *intégrité – elle est liée aux données qu'elle authentifie et, elle est créée dans des conditions qui permettent la conservation des données et le respect de leur intégrité; et (2) imputabilité --elle est imputable au signataire qu'elle identifie*." Unlike the Italian legislation, this definition neither requires the use of public key cryptography nor depends upon whether the signature is authenticated by a licensed CA. As the report later observes, "*toute signature électronique fiable doit être admise en preuve même si elle est assortie d'un certificat délivré par un tiers certificateur non accrédité.*"

form...." Significantly, however, the EU Directive adopts a relatively high standard for which "electronic signatures" benefit from this requirement of non-discrimination. The proposed Directive requires that an electronic signature (1) is uniquely linked to the signatory; (2) is capable of identifying the signatory; (3) is created using means that the signatory can maintain under his sole control; and (4) is linked to the data to which it relates in such a manner that any subsequent alteration of the data is revealed. This is a significantly more prescriptive and stringent standard than Article 7 of the UNCITRAL Model Law, and, at least at present, would appear to require the use of digital signature technology. Thus, the draft EU Directive will allow Member States to set a fairly high threshold for the types of electronic signatures that are not to be discriminated against because of their electronic form.

B. Legal presumptions

All of the provisions described above are generally intended to ensure that national laws do not discriminate against or otherwise discourage the use of electronic signatures. As discussed above, several jurisdictions have gone a step further and attached certain legal presumptions to the use of electronic signatures, such as a presumption of identity or intent to sign. Several jurisdictions also permit the use of electronic signatures in situations where the law would ordinarily require some enhanced form of authentication, such as a sworn, certified, or sealed document. The willingness of national legislatures to extend these benefits to digital signatures -- or at least those that are implemented according to prescribed standards -- reflects the extent to which digital signature technology is not only a reliable substitute for a handwritten signature, but is actually more reliable than a handwritten signature for many purposes.

The extent to which different jurisdictions have adopted or proposed these measures varies. As noted above, the proposed EU Directive provides that a "qualified certificate" -- *i.e.* one that is issued by a CA that satisfies the requirements of Annex II -- must be recognized by the Member States as satisfying the legal requirements of a handwritten signature, and must be admissible in legal proceedings in the same manner as handwritten signatures, so long as it was generated using a "secure signature creation device." The standards for a "secure signature creation device," as set forth in Annex III of the Directive, are very much in flux as of this writing. The standards that have been proposed would impose fairly broad requirements on signature creation devices, such as ensuring that the secrecy of a private key is "reasonably assured," and that it can be "reliably protected" by the legitimate holder. However, some Member States have sought to impose more stringent technical requirements on "secure signature creation devices," which might, for example, effectively require that all private keys be stored on smart cards. It is not clear, at this time, how this debate will be resolved.[116]

At first glance, the EU provision would appear to require the Member States to accept electronic signatures that satisfy the Annex II and Annex III criteria (whatever they turn out to be) in any situation where a handwritten signature is required by national law, including conveyances of real property, the formation of wills, and other such documents. Given that most Member States will want to retain at least some of these traditional signature requirements, the presumption accorded to qualified certificates appears exceptionally broad. At the same time, Article 1 of the Directive states that the Directive does not address "the conclusion and validity of contracts and other non-contractual formalities requiring signatures." This appears to be a significant exception to the requirement of granting legal equivalence to qualified certificates, and one that would permit Member States to retain many traditional writing requirements. Thus, it is unclear how these two provisions will interrelate.

---

116. As discussed below, another critical issue in the debate over Annex III is who would determine compliance with the Annex III standards, *e.g*, national governments, industry bodies, or the European Commission.

Under the Singapore Electronic Transactions Bill, documents that are signed by a secure electronic signature are entitled to a presumption of integrity, a presumption that the signature is that of the person with whom it is associated, and a presumption that the user affixed the signature with the intent of signing or approving the document. Significantly, the ETB does not limit these presumptions to electronic signatures that are confirmed by licensed CAs; the presumption also applies to any "commercially reasonable security procedure agreed to by the parties" and that satisfies the general criteria for uniqueness, identity, security, and integrity.

The Malaysian legislation provides that a digital signature confirmed by a licensed CA is entitled to a presumption that the signature belongs to the listed subscriber and that it was affixed with the intention of signing the message.

Some jurisdictions have concluded that electronic signatures, even ones that satisfy heightened standards of security and reliability, should not benefit from any special presumptions or powers. As the recent Australian report concluded, these sorts of presumptions "may involve incorrect guesses about efficient and fair business practices across a range of commercial contexts and may have serious unintended consequences.... The law should not seek to place addressees of electronically signed data messages in a better position than addressees of manually signed paper-based messages. Accordingly, at this stage legislated attribution rules should not go beyond restating the common law."

III. Licensing and accreditation of certificate authorities

For those jurisdictions that have specifically addressed the operation of a PKI, one of the central issues has been whether to require licensing of Certificate Authorities or, if not, whether to provide some other form of voluntary licensing or accreditation. As was evident in the preceding discussion of the legal effect of electronic signatures, and as will become evident in the subsequent discussion of liability, the extent to which the government exercises some sort of regulatory authority over CAs tends to influence legislators' willingness to grant specific legal benefits to CAs and the electronic signatures that they confirm. As discussed below, whether or not a particular jurisdiction requires CAs to obtain a license also has a direct effect on the operation of CAs within closed systems (*i.e.* systems in which all of the parties to an authenticated communication, including the CA, have previously defined their respective rights and obligations by contract).

Somewhat surprisingly, whether or not a particular country "requires" licensing of CAs is not always clear. Article 4(3) of the Malaysian legislation, for example, appears to require any certificate authority confirming the validity of a digital signature in Malaysia to be licensed by the Controller of Certificate Authorities, on pain of criminal prosecution. At the same time, Article 13 provides that a digital signature will not be denied legal effect simply because it was confirmed by an unlicensed CA. The paradoxical result is that the legislation would apparently accept the legal validity of a digital signature confirmed by an unlicensed CA, but then subject that CA to criminal prosecution. Thus, it is simply not clear whether Malaysia's licensing scheme is truly "mandatory."

The Italian legislation, as well as the recently-published draft implementing regulations, establishes a mandatory licensing scheme for all CAs, although this result is evident more by implication than by express provision. CAs are obligated to register with the Italian Authority for Information Technology in Public Administration (AIPA), and must comply with extremely specific (and generally quite stringent) financial and technical standards. For example, CAs must have a registered share capital of approximately

USD 7.5 million, and must satisfy character and fitness requirements similar to those imposed on bank personnel.

Germany's licensing system is at least nominally voluntary, in that it permits "the application of [unlicensed] digital signature procedures ... insofar as digital signatures ... are not legally required under the [digital signature] law." At the same time, the law and the associated draft technical regulations clearly contemplate that all CAs will be licensed by the national "root" CA, and at least one commentator has observed that the stated intent of German officials is to create a *de facto* mandatory licensing regime.[117]

The Singapore Electronic Transactions Bill, while not requiring CAs to be licensed, imposes a number of requirements on CAs without regard to whether they are licensed. For example, all CAs, licensed or unlicensed, must either issue a Certification Practice Statement or abide by the statutorily-prescribed requirements for issuing a digital certificate. Additionally, all CAs must comply with statutory standards for disclosing material information about a certificate and the procedures for revoking or suspending a certificate. As noted above, Singapore provides certain presumptions of attribution and intent both to licensed CAs and to others who satisfy the prescribed criteria, but only permits licensed CAs to state liability limitations in their certificates.

Significantly, the EU draft Directive prohibits Member States from requiring licensing of CAs. (This provision, if adopted, will likely have a significant effect on the Italian and, to a lesser extent, the German regulatory schemes.) At the same time, the Directive allows Member States to adopt voluntary licensing schemes, provide that those schemes are "objective, transparent, proportionate, and non-discriminatory."

Interestingly, the two benefits that accrue to "qualified certificates" under the Directive -- legal equivalence to a hand-written signature and the right of the issuing CA to limit its liability -- do not turn, and in fact may not turn, on whether the CA is licensed or accredited. The sole requirements are that the CA satisfy the standards for qualified certificates in Annex I, the operational standards for CAs set forth in Annex II, and, with regard to legal recognition, the standards for "secure signature creation devices" set forth in Annex III. In practice, however, there may be very little distinction between satisfying these standards and becoming licensed or accredited. With regard to Annex III, for example, the Member States are continuing to debate how individual CAs would certify their compliance with the relevant standards. The proposals on the table range from self-certification by the CA to elaborate testing and certification mechanisms administered by national governments and/or the European Commission. Others have proposed that appropriate industry organizations would have the power to certify compliance with the Annex III standards. Similar certification issues are raised by the Annex II standards concerning the operational requirements for CAs.[118] Depending on how these issues are resolved, a CA that wanted to assure the legal equivalence of its electronic signatures might have no practical choice but to undergo one or more testing and accreditation process.

---

117. See *Draft of the Digital Signature Ordinance*, translation and commentary by Christopher Kuner, available at www.kuner.com. To take one example of how the German legislation effectively mandates licensing, Section 13(4) states that, if a CA's license is withdrawn of revoked, the CA "shall ensure transfer of the activity to another certification authority or winding up of the contracts with the owners of the signature keys." The clear implication of this provision is that if a CA no longer has a license, it can no longer have customers. If licensing is voluntary, however, why would the loss of a license result in what amounts to an obligation to cease doing business?

118. For example, Annex II requires CAs to "demonstrate the reliability necessary for offering certification services." Naturally, this raises the question "demonstrate to whom?"

While the apparent assumption in many jurisdictions has been that the government will act as the licensing or accreditation authority (whether as part of a mandatory or voluntary regime), there is growing recognition that private sector organisations, or other types of standards bodies, may be better suited to this role. The Netherlands, for example, recently established a voluntary "TTP Chamber" that brings together government and commercial representatives. The TTP Chamber serves, in effect, as a standards-setting organisation for the use of electronic signatures in the Netherlands, and CAs are strongly encouraged (but not required) to join. The Netherlands adopted this approach, in part, because it concluded that an organisation of this nature would be better equipped to respond to rapidly changing market and technological forces.[119]

IV. Liability

A. Background

One of the most complicated issues surrounding the creation of a public key infrastructure is the extent to which the law should define or limit the liabilities of the three main parties to a secure electronic transaction, that is, the person who digitally signs a message, the person who receives the message and who may rely on its validity, and the CA that vouches for the identity or some other attribute of the sender. In a purely "open" transaction -- that is, one in which the parties have not previously defined their respective rights and duties by contract -- there are several major faultlines of liability. Most importantly, the CA may be liable to the recipient of the message for any inaccuracies or misrepresentations contained in the certificate, or for the failure of the CA to revoke an invalid certificate. To take a simple example, a person who applies for a digital certificate may misrepresent his or her identity under circumstances where the CA, with more thorough investigation, could have discovered the deceit. When a third party relies on that certificate to its detriment, to what extent is the CA liable? Given that the CA and the third party do not necessarily have a pre-existing relationship in which they have had an opportunity to allocate this sort of risk, they must turn to general legal principles to define the scope of the liability. Moreover, given the high value of transactions for which digital signatures might be used, the CA's potential liability is quite steep.

It is this central feature of an open PKI that was responsible for much of the initial legislative interest in digital signatures. One of the early rationales for digital signature legislation was that, in the absence of a legislatively-imposed limitation on the CA's potential liability, this method of electronic authentication would never emerge in the marketplace, to the detriment of electronic commerce generally. More recently, however, at least one commentator has observed that if a CA cannot operate without a legislatively-imposed limitation on its liability, it is not a business that can internalize its own costs, and therefore not one that should be brought into existence by legislative fiat.[120] Critics contend that, in effect, a legislative

---

119. Along the same lines as the Dutch model, a recent discussion paper issued by the Australian National Office for the Information Economy proposed the creation of a "National Authentication Authority" that would not serve as a root CA, but that would develop industry codes of practice and issue "quality labels" to best practice organisations and systems.

120. See, e.g. *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*, available at www.w3journal.com/7/s3.biddle.wrap.html.

limitation on liability merely shifts the risk of loss to third parties who may rely on an inaccurate digital certificate.[121]

B. National Approaches

Three jurisdictions -- the EU, Malaysia, and Singapore -- have addressed the potential liability of CAs. Significantly, all three jurisdictions have taken an approach that combines some variant of strict liability for certain acts or misrepresentations with a system that permits the CA to limit its liability, at least under certain circumstances.[122] Malaysia and Singapore, for example, require CAs to specify a "recommended reliance limit" in any certificate that they issue. The recommended reliance limit then sets a cap on the CA's potential liability for losses caused by reliance on a misrepresentation in the certificate of any fact that the CA was required to confirm, or as a result of any failure to comply with the statutorily-prescribed requirements for issuing a certificate. Similarly, while the EU Directive generally imposes strict liability on a CA for losses caused by reliance on an inaccurate certificate or failure to abide by the requirements for issuing a qualified certificate, Member States are required to permit CAs to specify the permissible uses of a qualified certificate and the maximum value of any transaction for which it may be used.[123] In effect, these schemes permit the CA to define the value of a particular certificate in the manner described above.

These jurisdictions differ on whether licensing or accreditation is a prerequisite to a limitation on liability. Singapore and Malaysia only permit licensed CAs to state liability limitations in the certificates that they issue. The EU would permit any CA that issues a "qualified certificate" to limit the permissible uses of that certificate or to specify its maximum value. As discussed above, the draft Directive would permit unlicensed CAs to issue qualified certificates, but the practical reality is that most CAs that issue qualified certificates will be licensed or accredited under voluntary schemes.

Some jurisdictions have chosen not to address the liability issues associated with an open PKI. Germany, for example, has so far avoided any effort to legislate liability provisions for the operation of a PKI, and has actively opposed the liability limitation provision of the draft EU Directive (which, if adopted, would compel Germany to allow CAs to limit their liability). Many German lawyers and policy makers believe that existing principles of liability under German law adequately address the issues raised by an open PKI,

---

121. If legislation permits CAs to limit their liability, however, it would seem that the market would quickly determine the appropriate range of certificate values and their corresponding costs to users. If there is demand for high value certificates with correspondingly high liability limitations, a CA would presumably charge the holder of the certificate an amount that includes an appropriate risk premium and thereby internalise its costs. Similarly, if there is demand for low value or even "no value" certificates which many believe will be the most widespread use of digital signatures the CA would limit its liability to an appropriately small amount (and perhaps forego liability altogether), and the cost to the user would be reduced. The only real hazard of this market driven approach is that third parties will have to be diligent in confirming the validity of a certificate, and the acceptability of any liability limitation it contains, in light of the nature of the transaction. As the value of a transaction increases, however, it seems presumptively more reasonable to impose those duties on third parties. Moreover, if it turns out that the risks for third parties remain too great, they will not accept high value certificates and no market for these certificates will emerge.

122. The Japanese ECOM Guidelines are less clear, stating in paragraph 2.2 that "Each certification authority should define in its [Certification Practice Statement] its level of responsibility and compensation for losses resulting from its breach of obligation, taking into account any applicable regulations and other factors." This would appear to permit CAs to limit their liability, although this result is not entirely clear.

123. The draft UNCITRAL Uniform Rules adopt a similar scheme. At the time of writing, however, the UNCITRAL Working Group had not yet had a chance to consider the liability issue fully.

and oppose the introduction of a system that is based on strict liability and that would permit CAs to state liability limitations. The recent Australian report noted the debate surrounding liability limitation provisions, and concluded that it would be premature to address the issue until "the technology develops and market issues and failures emerge…." Neither the Italian legislation nor the recent French report addresses liability issues.

At this stage, then, it is hard to identify a strong international consensus on the liability aspects of an open PKI. Some countries apparently believe that allowing CAs to limit their liability is a prerequisite to the widespread use of electronic authentication, while others believe that such a limitation is either unnecessary or premature. This lack of consensus may prove to be a significant obstacle to the formulation of international standards on electronic authentication, whether by means of the UNCITRAL Uniform Rules or an international convention.

V. Closed systems / Party autonomy

A. The growing significance of closed systems

When digital signature technology first began to emerge, it was widely assumed that its principal use would be in "open" transactions, *i.e.* transactions in which the parties have not agreed in advance on their respective rights and duties in using that technology. Indeed, as discussed above, one of the principal motivations for digital signature legislation has been to define the rights, duties, and potential liabilities of the three central parties to a secure electronic transaction: the person who sends an authenticated message, the person who receives the authenticated message, and the CA that confirms the validity of that message.

More recently, however, it has become evident that many, if not most, applications of digital signature technology will be in "closed" environments, *i.e.* situations in which all of the relevant parties have agreed in advance on their respective rights and duties, and allocated any potential risks. For example, a company can issue digital signatures to all of its employees for purely internal use, with the company acting as its own CA and setting its own rules. More significantly, digital signatures can also form the basis for a secure electronic payment system, including the Secure Electronic Transaction (SET) specification developed by Visa, Mastercard, and other members of the payment card industry. In SET, each of the parties to a secure electronic transaction -- the cardholder, the merchant, and the member banks that process the transaction -- has a digital signature that establishes its identity and authority within the system. As in an ordinary payment card system, the parties' rights and duties are established by a series of contracts.

Because the parties to a closed transaction have already defined the terms and conditions for using digital signatures amongst themselves, there is a significantly reduced need for legislative intervention. Liability, for example, can be agreed upon by the parties in advance. Indeed, the greatest risk faced by users of closed systems is that legislation will fail to recognize the terms of their private agreements, or impose unnecessary regulatory burdens and costs on their use of digital signatures. Given that the use of electronic signatures within closed systems is likely to predominate over the use of electronic signatures in "open" transactions, it is extremely important that legislation not inhibit the continued development of closed systems.

B. Factors that affect closed systems

1. Licensing

The extent to which electronic authentication legislation recognizes and accommodates closed systems is a function of several different factors. For example, legislation that requires licensing of all CAs or that establishes other types of requirements for unlicensed CAs is likely to impose a significant burden on closed systems, because it may require the CA to become licensed in multiple jurisdictions or to abide by standards that are different from those to which the parties have agreed. As discussed above, while only Italy has apparently imposed a licensing requirement for all CAs, several jurisdictions have adopted legislation that creates a *de facto* mandatory licensing regime or that imposes standards on unlicensed CAs. These provisions run the risk of significantly increasing costs for the operators of closed systems.

2. Permitting contractual departures from prescribed standards

At the simplest level, the most important accommodation for closed systems is to state that the standards and requirements established by electronic authentication legislation or policies do not affect the terms of private agreements concerning the use of electronic signatures. To date, no jurisdiction has made this statement explicitly, although it may be implicit to some degree in legislation that does not require licensing of CAs. This is not to say that legislation can, or should, treat closed systems equally. As discussed above, several jurisdictions have adopted certain presumptions that apply only to electronic signatures authenticated by licensed CAs, or to electronic signatures that satisfy statutorily-prescribed criteria. Similarly, the right of a CA to limit its liability will often depend on whether or not it is licensed or accredited. In practice, these distinctions should not have a significant effect on closed systems, because these are precisely the types of issues that can be addressed by contract among the parties. What is important is that legislation not preclude these types of agreements among parties.

3. Giving effect to electronic signatures in closed systems

To the extent that legislation addresses the legal effect of electronic signatures, it is also important to ensure that the legislation accords at least a minimum degree of legal recognition to electronic signatures used within closed systems, such that they can be proven in court in accordance with whatever standards would ordinarily apply. Of those jurisdictions that have addressed the legal effect of electronic signatures, only Italy would appear to deny legal effect, or at least not to affirmatively grant legal effect, to electronic signatures used within unlicensed closed systems. As noted above, the draft EU Directive would prohibit Italy and other Member States from denying legal effect to an electronic signature solely on the grounds that it is in electronic form, which would provide at least some legal clarity to the use of electronic signatures within closed systems. Moreover, signatures that are verified by a "qualified certificate" within a closed system and that are executed with a "secure signature creation device" would be entitled to legal equivalence to a handwritten signature.[124]

4. Accommodating non-identity, or "Authority," certificates

From the standpoint of closed systems, it is also important that legislation recognize the legal effectiveness of signatures that establish some authority or attribute of the signer, rather than the signer's personal

---

124. However, as discussed above, a closed-system CA seeking to benefit from the presumption of legal equivalence under the EU Directive may need to undergo certification processes with respect to the Annex II and Annex II.I standards.

identity. Although this issue is not unique to closed systems (because there may very well be a market for various kinds of "authority certificates" on open systems), electronic signatures that are used within a closed system are considerably more likely to certify authority than identity. In a secure electronic payment system, for example, the signature confirms the signer's authority to use a particular credit card number, but does not necessarily establish the signer's identity. Electronic signatures may also be used in hardware and software components to identify a device or to prevent copyright offences, and industries that rely on these techniques would like such signatures to have evidential weight.

The draft EU Directive raises a particular concern, in this regard, because it requires qualified certificates to be linked to "the unmistakable name of the holder or an unmistakable pseudonym." Because the Directive would only obligate Member States to give full legal effect to qualified certificates, the result is that Member States would apparently not have to give legal effect to non-identity certificates in judicial proceedings even if they otherwise satisfied the requirements for a qualified certificate. Similarly, Singapore defines a "secure electronic signature" as one that, *inter alia*, is capable of identifying the signer. The effect of these provisions will be to make it more difficult, if not impossible, to establish the legal validity of non-identity certificates and to enforce transactions that are authenticated by non-identity certificates.

VI. Cross-border recognition

One of the greatest risks posed by the current flurry of legislative interest in electronic signatures is that national legislation will actually inhibit the use of electronic signatures in international commerce. There are two distinct but closely interrelated ways in which this could happen. First, if electronic signatures and the CAs who authenticate them are subject to conflicting legal and technical requirements in different jurisdictions, it may be difficult or impossible to use electronic signatures in many cross-border transactions, simply because the conditions for their use have not been satisfied in one or more jurisdictions. These are substantive conflicts that many believe give rise to the need to harmonize international standards.

The second way in which legislation can inhibit the use of electronic signatures in international commerce (and the subject of this section) is the means by which national authorities grant recognition to foreign electronic signatures and certificates. So far, every jurisdiction to consider the matter has incorporated some assessment of the standards adhered to by the foreign CA, so the issue is inextricably related to the broader question of conflicting national standards. At the same time, legislation may also impose other geographic or procedural limitations that prevent cross-border recognition of electronic signatures.

Licensing requirements are a pivotal issue. To the extent that a jurisdiction requires a CA to be licensed, or to adhere to particular standards notwithstanding its status as a licensee, this could be construed to mean that any CA that issues a digital certificate in that jurisdiction -- or that even confirms the validity of a digital certificate to someone in that jurisdiction -- is required to abide by those conditions.[125] This raises the possibility that a CA would have to obtain licenses in many different jurisdictions, which would certainly be costly and could very well be impossible in particular circumstances, if licensing conditions were not substantially the same.

---

125. There are, of course, significant conflicts of laws and jurisdictional issues related to the power of a national government to exercise authority over a foreign CA under these circumstances.

The Malaysian legislation, for example, could be interpreted to require any CA operating in Malaysia to be licensed. As discussed above, however, the legislation also contains provisions that appear to recognize the legality of unlicensed CAs. Thus, it is simply not clear whether an unlicensed foreign CA would be subject to possible criminal prosecution for issuing or validating a digital certificate in Malaysia. The Malaysian legislation also provides that the Controller of Certificate Authorities may recognize CAs "licensed or otherwise authorised by governmental entities outside Malaysia that satisfy the prescribed requirements." Thus, to the extent that Malaysia would recognise foreign CAs at all, it would only do so for regulated foreign CAs -- thereby denying recognition to unlicensed CAs or CAs from jurisdictions that have chosen, as a matter of policy, to forego any licensing scheme for CAs.

In the case of Italy and Germany, both geography and standards pose potential obstacles to cross-border recognition. The Italian legislation limits cross-border recognition to foreign CAs that satisfy "equivalent requirements" and that are from another EU Member State or from a member state of the European Economic Area ("EEA"). Thus, foreign CAs outside of the EU and EEA cannot be recognized. Similarly, the German legislation recognizes foreign certificates so long as the issuing CA is from an EU or EEA Member State and has demonstrated "an equivalent level of security." Because Germany has adopted extremely stringent technical standards for the use of digital signatures -- for example, by requiring that private keys be stored on smart cards -- many foreign CAs will be unable to demonstrate "an equivalent level of security." The German legislation also provides that foreign CAs may be recognized pursuant to an international agreement.

In time, both the Italian and German provisions are likely to be overtaken by whatever cross-border provision the EU ultimately adopts in its electronic authentication directive. At present, the draft EU Directive provides that a Member State must recognize a foreign CA if (1) the foreign CA has been accredited under a voluntary licensing scheme established by a Member State; (2) a CA established in a Member State guarantees the foreign CA's certificates to the same extent as its own; or (3) the foreign CA is recognized by an international agreement between the EU and a third country or countries. This provision is significantly more accommodating than the German and Italian legislation, but would still require a foreign CA either to become accredited in a Member State or to enter into a cross-certification arrangement with an accredited CA (absent an applicable international agreement to the contrary).

VII. International initiatives

The problem of cross-border recognition directly implicates the broader question of whether the international community should adopt international standards concerning electronic authentication, and the means by which it should do so. Divergent national standards, as well as other types of regulatory obstacles, are likely to cause a significant drag on the use of electronic signatures in global electronic commerce. Uncertainty concerning the legal effect of electronic signatures, conflicting licensing regimes, conflicting operational and technical requirements for CAs, uncertain liability exposure -- all of these factors are likely to impede the cross-border use of electronic signatures. Several initiatives are underway to develop international standards to overcome these obstacles.

1. European Union Draft Directive

The most significant of these initiatives, and one that has been discussed throughout this paper, is the EU draft Directive on Electronic Signatures. If adopted in its present form, the Directive would obligate the 15 members of the European Union to enact national legislation implementing the Directive's requirements by 1 January 2001. The Directive would harmonise national policies concerning electronic authentication and the recognition of electronic signatures across a diverse range of national legal systems. Although the

Directive is not yet final, it has already had a significant impact on those Member States that are actively considering electronic authentication legislation. Some countries have apparently decided to await the final outcome of the Directive before considering national legislation. At the same time, there remain significant differences of opinion over the Directive -- including, for example, the means by which CAs would certify their compliance with the Annex II and Annex III standards -- so it is by no means certain what the final contours of the Directive will be.

2. UNCITRAL

In December 1996, UNCITRAL adopted the Model Law on Electronic Commerce to create a general framework for paperless transactions. As discussed above, Article 7 of the UNCITRAL Model Law establishes a broad, criteria-based standard for the recognition of electronic signatures as equivalent to handwritten signatures, and that provision has proven influential in several jurisdictions.

Building upon that work, the UNCITRAL Working Group on Electronic Commerce is now developing uniform rules that relate more specifically to electronic signatures and the operation of certificate authorities. As discussed above, the current draft of the UNCITRAL uniform rules adopts the two-tier approach to electronic authentication legislation, giving legal effect to a broad class of electronic signatures while granting more specific presumptions to electronic signatures that satisfy more stringent criteria. The Working Group continues its consideration of uniform rules for the operation of certificate authorities, including issues related to liability, operational requirements for CAs, and standards for cross-border recognition.

Recently, the Working Group has also started to consider an alternative draft set of uniform rules, WP.80, which would limit itself to a minimal set of requirements designed to give legal effect to electronic signatures. WP.80 is, in fact, part of an effort to bridge some fairly significant differences of opinion among the countries participating in the UNCITRAL talks. As of this writing (early February, 1999), it is impossible to predict whether WP.80 or some other initiative will be sufficient to hold the UNCITRAL talks together and produce a final set of rules.

3. Proposed international convention

While the UNCITRAL process has proven extremely worthwhile, its objective is to develop uniform rules that governments may consider -- but are by no means obligated to adopt -- when drafting national legislation. In contrast, an international convention would bind signatories to recognise the principles and requirements contained in it. The United States Government has circulated an early draft of such a convention, and several other governments have expressed support for the idea.

4. Organisation for Economic Co-operation and Development

In conjunction with the Ottawa Ministerial meeting on electronic commerce, held in October 1998, the OECD issued a comprehensive inventory of electronic authentication legislation and policies in the OECD Member countries, and adopted a Declaration on Authentication for Electronic Commerce. The principles set forth in the Declaration generally encourage electronic authentication policies that minimise

government regulation, support technological neutrality, and recognize party autonomy.[126] The Declaration also recognizes "the potential impact that diverse national solutions for electronic authentication could have on the development of global electronic commerce," and encourages countries to "take a non-discriminatory approach to electronic authentication from other countries."

The OECD is continuing its work in this area through this Workshop.

5. Other international organisations

In addition to UNCITRAL and the OECD, a number of other international organisations have been involved in international electronic authentication issues:

- The International Chamber of Commerce has issued a General Usage for International Digitally Ensured Commerce ("GUIDEC"), which attempts to create a general framework for the use of digital signatures in international commercial transactions (*i.e.* for international business-to-business transactions). GUIDEC seeks to draw upon existing law and practice in different legal systems to identify and promote general principles for the use of digital signatures in international commerce.

- The Public Key Authentication Task Group of Asia-Pacific Economic Co-operation (APEC) issued a preliminary report in September 1997, which surveys the range of issues associated with electronic authentication legislation and recommends international co-ordination in numerous areas to avoid interoperability and trade obstacles.

126. For example, the Declaration recognizes that "transacting parties may select appropriate mechanisms which meet their needs for authentication in conducting electronic commerce, including particular authentication technologies, contractual arrangements and other means of validating electronic transactions, and that they can use judicial and other means of dispute resolution to prove the validity of those transactions."