Unclassified **DSTI/ICCP/REG(99)6/REV1**

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

OLIS : 11-Aug-1999
Dist. : 11-Aug-1999

Or. Eng.

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

DSTI/ICCP/REG(99)6/REV1
Unclassified

Working Party on Information Security and Privacy

JOINT OECD-PRIVATE SECTOR WORKSHOP ON ELECTRONIC AUTHENTICATION

BACKGROUND PAPER ON ELECTRONIC AUTHENTICATION TECHNOLOGIES AND ISSUES

Stanford and Menlo Park, California, 2-4 June 1999

This document is a reivsed version of the background paper drafted for the Joint OECD-Private Sector Workshop on Electronic Authentication. It was drafted by Stewart Baker and Matthew Yeo of Steptoe and & Johnson, LLP in consultation with the OECD Secretariat, taking into consideration comments received from members of the Working Party on Information Security and Privacy (WPISP). At its meeting on 5 June 1999, the WPISP agreed that the Proceedings of the Workshop, of which this document is part, also be made available on the OECD Website at http//www.oecd.org/dsti/sti/index.htm.

Mr. Taizo Nakatomi,
Tel: (33 1) 45 24 96 93, Fax: (33 1) 45 24 93 32
Email: taizo.nakatomi@oecd.org

80496

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

Or. Eng.

BACKGROUND PAPER ON ELECTRONIC AUTHENTICATION TECHNOLOGIES AND ISSUES

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.*[1] “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 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 email 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.[2]

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?

[1] 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.

[2] 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.

– 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 aspects of a 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 email to engage in precisely these sorts of communications. While a standard email program has none of the types of secure authentication features discussed below, the fact that one can associate an email 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 email message could also be sufficient to establish the person's intent to 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 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 email addresses; email directories are seldom consulted to confirm that the email address used is truly connected with a particular individual or entity.[3] 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

[3] Email 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 email address such as joe.smith@oecd.org.

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 email, 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 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 on-line banking customers. In such a system, a customer's online banking log-in, passcode, and fingerprint are stored on a chip that is attached to a multi-application smart card. An on-line 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 the 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.[4] Certification authorities could utilise a variety of technologies to

[4] 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 purposes of this paper, the term certification authority is applied to the broader concept of a public or private sector

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 is 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 that 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 that 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 that 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 bear 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 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

entity that acts as an independent trusted source for certifying many kinds of information in the electronic environment.

which it is incorporated (if it is an incorporated entity) and its principal place of business. “Attributes” encompasses 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 adheres 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.”[5] 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 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 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 her 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

[5] 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 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.

"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 email 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 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 predetermined 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 in the 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.[6] Where possible,

[6] 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

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?
- 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

consideration under each session. The workshop itself did not cover individual-to-individual communications, because it was focused on electronic commerce applications. However, an examination of 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.

technology is being used. Turning first to business-to-individual applications, the following examples illustrate some of the broad use 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, are airline frequent flyer programs. 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" Programs***. "Seal" programs 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 program 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 of 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 or 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.