

CHAPTER 9

CRYPTOGRAPHY AND ELECTRONIC SIGNATURES

Maury D. Shenk, Stewart A. Baker, and Winnie Chang
Steptoe & Johnson LLP
London, England and Washington, DC, United States

9.01 Introduction

The use of mathematical and other techniques to scramble and unscramble information — known as cryptography or encryption — has a long and fascinating history. One of the better-known examples of early cryptography is the Caesar cipher, a simple method that Julius Caesar is said to have used to secure confidential communications to his army.

While protecting access to secret information is still a major reason for using cryptography today, cryptographic techniques also are increasingly used to authenticate the identity of individuals and to ensure data integrity (i.e., the assurance that information has not been altered in storage or transit between a sender and intended recipients).

Modern encryption technology is based on several types of mathematical algorithms — primarily symmetric algorithms, asymmetric algorithms, and hash algorithms. Although these algorithms are highly complex, a brief description is appropriate.

Symmetric algorithms (such as AES, DES, and Blowfish) allow confidential communications using a secret “key” shared by the sender and recipient. Asymmetric algorithms (such as RSA, ElGamal, and Diffie-Hellman) involve two mathematically related keys, one of which is usually public. Asymmetric algorithms can be used both for confidentiality (via encryption with the recipient’s public key and decryption with the recipient’s private key) and digital signature (via signature with the sender’s private key and verification

with the sender's public key). Hash algorithms (such as SHA-1 and MD5) take a variable-length message (as short as a sentence or as long as a book) and produce a unique, fixed-length "digest" that can be used to confirm that the message has not been changed.

Particular practical applications of encryption (on the Internet, other networks, and otherwise) often involve complex combinations of these encryption algorithms into encryption "protocols", such as SSL (for secure connections over the World Wide Web), S/MIME (for secure email), IPsec (for securing Internet TCP/IP traffic), and others.

9.02 Regulation of Encryption: Export, Import, and Use

(a) In General

With the growth of the Internet as a global communications infrastructure, encryption has become the subject of debate and government regulation in recent years. On the one hand, encryption software and hardware allow individuals to send and receive secure, authenticated communications, thus providing important benefits that include protection of legitimate privacy interests and enhanced viability of electronic commerce.

On the other hand, there is ongoing concern that encryption could potentially allow criminals, terrorists, and unfriendly governments to hide their communications and illegal activities. As a result, many countries tend to apply strict regulation to encryption products.

(b) Types of Encryption Regulation

(i) General Principles and Exceptions

Confidentiality vs. Authentication As mentioned above, encryption can be used to provide confidentiality (i.e., the assurance that only authorized persons have access to secret information) and/or authentication (i.e., a trusted way to verify the identity of a particular person who sent a specific message, commonly through the use of electronic signatures).

Most countries today only restrict items that use encryption for confidentiality.

Temporary Import and Export Many countries exempt temporary encryption import and export for "personal use" (usually including business uses), allowing travelers to carry personal laptops loaded with encryption software into and out of the country without any special license or authorization.

Intangible Transfers The United States and many European Union (EU) member states control intangible transfers (i.e., Internet downloads and uploads) of

encryption technology quite aggressively. In the recent climate of heightened electronic vigilance, other countries (e.g., Singapore) have decided to follow suit.

However, some countries (mainly in South America, Africa, and the Middle East) do not extend import and export controls to intangible transfers of encryption software, and generally due to the focus of their customs laws on physical items.

(ii) Export

Established in July 1996, the Wassenaar Arrangement was designed to increase the transparency and responsibility in global transfers of conventional arms and dual-use goods and technologies.¹ It is one of several worldwide non-proliferation regimes created near the end of the Cold War. Other principal regimes are the Nuclear Suppliers Group, the Australia Group, and the Missile Technology Control Regime, and they are mainly directed against the proliferation of weapons of mass destruction and missiles. The 33 participating countries of the Wassenaar Arrangement are:

1. Argentina;
2. Australia;
3. Austria;
4. Belgium;
5. Bulgaria;
6. Canada;
7. Czech Republic;
8. Denmark;
9. Finland;
10. France;
11. Germany;
12. Greece;
13. Hungary;
14. Ireland;
15. Italy;
16. Japan;
17. Korea, Republic;

¹ See <http://www.wassenaar.org>.

18. Luxembourg;
19. The Netherlands;
20. New Zealand;
21. Norway;
22. Poland;
23. Portugal;
24. Romania;
25. Russian Federation;
26. Slovakia;
27. Spain;
28. Sweden;
29. Switzerland;
30. Turkey;
31. Ukraine;
32. United Kingdom; and
33. United States.

Membership is open on a global and non-discriminatory basis to countries meeting certain criteria. In particular, a country must:

1. Be a producer or exporter of arms or associated dual-use goods and technology;
2. Maintain non-proliferation policies and appropriate national policies (including adherence to international non-proliferation regimes and treaties); and
3. Implement fully effective export controls.

The member countries agreed to control all items on the Wassenaar Arrangement Munitions and Dual-Use lists, with the aim of preventing unauthorized transfers or re-transfers of those items. These lists are reviewed periodically to take into account technological advances or other changes. The Dual-Use List consists of a basic list (tier 1) and annexes of sensitive (tier 2) and very sensitive (sub-set of tier 2) items. Most encryption hardware, software and technology are in tier 1, although cryptanalytic items (i.e., those designed for “breaking” encryption codes) are designated as sensitive items.

Although the Wassenaar Arrangement sets out the minimum standards for export regulations for military and dual-use goods (including encryption

items), member countries are allowed to authorize exports according to their own policies and discretion.

With respect to encryption controls, the Wassenaar Arrangement explicitly provides exclusions for mass-market products, weak encryption (with key length up to 56 bits), mobile telephones, personalized smart cards, digital signature products, equipment used for banking transactions, copy protection software, and other items.

National Practices Australian, Canadian, EU, Japanese, and United States export controls are closely based on Wassenaar controls.

Although Hong Kong and Singapore are not signatories to the Wassenaar Arrangement, they implement encryption regulations that generally follow Wassenaar guidelines. Other countries, including China, Israel, and Kazakhstan, apply various *ad hoc* controls.

(iii) Import

There are various types of import controls on encryption products. Some countries (including China, Tunisia, and certain former Soviet Union republics, such as Russia, Kazakhstan, and Uzbekistan) apply blanket import restrictions encryption items.

Some countries, such as Hong Kong and certain new EU members, such as the Czech Republic, Latvia, Lithuania, and Slovakia, apply Wassenaar restrictions to imports. Countries that do not implement encryption-specific import restrictions (e.g., Malaysia) may impose import and equipment type-approval requirements on telecommunication products (including any embedded encryption software or hardware).

(iv) Use

There also are various types of controls on the use of encryption products. Countries that apply blanket import prohibitions on encryption items (such as China, Tunisia, and Russia) usually have broad restrictions on encryption use. Certain countries (e.g., India) apply encryption-use restriction in particular applications (e.g., telecommunications and the Internet).

Other countries (including Israel and South Africa) implement restrictions on particular activities (e.g., commercial supply and development of encryption products and services) or pursuant to specified license conditions.

(c) Global Regulation

(i) In General

This section describes the encryption laws and policies of a sample of several countries (and the EU). The countries covered include leading producers of

encryption products, important markets for encryption products, and other countries whose laws illustrate the nature of global encryption regulation.

(ii) *United States*

United States export and re-export controls are administered by the Bureau of Industry and Security of the United States Department of Commerce. The Export Administration Regulations,² which contain rules governing exports of encryption items, apply to most products using encryption for confidentiality, except to certain products decontrolled under the Wassenaar Arrangement and products using “short-range wireless encryption”.

However, Bureau of Industry and Security regulations do not apply to encryption used for authentication, digital signature, or access control, or to exports to Canada. Exports of publicly available source code also are substantially decontrolled.

The strictest export treatment applies to encryption technology, proprietary source code, and open cryptographic interfaces exported to countries other than the favored countries (EU member states, plus Australia, Japan, New Zealand, Norway, and Switzerland).

Most encryption products are exportable under a license exception. Qualification for most license exceptions requires submission of a “review request” to the Bureau of Industry and Security. The request, which also is reviewed by the National Security Agency, is submitted on a Bureau of Industry and Security form and should also include a letter of explanation and technical specifications. A few encryption items — primarily network infrastructure and certain other products exported to foreign government entities and open cryptographic interfaces and encryption technology to non-favored countries — continue to require licenses from Bureau of Industry and Security.

Application procedures are similar to those for review requests, but license applications are reviewed by the Bureau of Industry and Security, the National Security Agency, the Federal Bureau of Investigation, the Department of State, and the Department of Defense.

Processing of review requests by the US government generally takes approximately four to eight weeks, although most products may be exported either immediately on submission of a review request or 30 days after the request is registered by the Bureau of Industry and Security. Processing times for license applications vary depending on complexity. The Bureau of Industry and Security requires post-export reporting for many encryption exports (as well as re-exports from Canada), but there are a variety of significant exceptions.

2 15 Code of Federal Regulation, sections 730–774.

The United States does not restrict the import or use of encryption products, although US legislation regarding wiretaps can affect use of encryption. For example, United States law enforcement agencies can, with appropriate judicial authorization, conduct electronic surveillance of electronic communications, under both federal and state law. This authority was significantly broadened by the USA PATRIOT Act,³ which was passed in response to the 11 September 2001 terrorist attacks on the United States.

To facilitate such electronic surveillance, telecommunications carriers are required by the Communications Assistance for Law Enforcement Act⁴ to build their networks in a way that facilitates wiretapping of publicly available telecommunications services. The use of encryption on telecommunications carrier networks may be affected by the obligations of Communications Assistance for Law Enforcement Act.

(iii) European Union

Majority Position The EU Dual-Use Regulation,⁵ originally passed in 2000 and modified several times since, has removed almost all restrictions on the intra-Community transfer of encryption products and technology, allowing the unlicensed shipment between EU member states of all encryption goods except cryptanalytic items.

Under the Regulation, the export of encryption goods or technology with key lengths greater than 56 bits generally requires authorization for all destinations outside the EU, though there are some significant exceptions to this rule. Among the primary exceptions, exports of all encryption products, except cryptanalytic items, are permitted under a General License to a group of seven favored countries: Australia, Canada, Japan, New Zealand, Norway, Switzerland, and the United States.

In addition, mass-market encryption products, regardless of key length, may be freely exported outside the EU, and no restrictions apply to the export of encryption goods and technology that are used for basic scientific research that provide the minimum information necessary for patent applications, or that are in the public domain. However, EU member states may impose additional controls on the products listed in the EU export control lists (even those deemed acceptable for intra-Community transfers) “to safeguard public policy or public security”. All encryption goods and technology not exempted from control must be licensed prior to export from any EU member state.

3 Pub. Law Number 107-56 (2001).

4 Pub. Law Number 102-414 (1994).

5 Regulation 1334/2000/EC.

An individual export authorization is generally required for the export of controlled encryption goods and technology outside the EU. Notably, the EU Dual-Use Regulation provides for General Licenses and other simplified procedures for the export of dual-use goods to the seven states listed above. The EU also permits global authorizations to be issued to a particular exporter for a type or category of dual-use goods and technology that may be eligible for export to one or more specified countries. The member states, and not the EU, have the authority to issue export licenses.

However, the EU has identified a number of factors that member states must take into account when issuing export authorizations, including commitments under other international agreements on non-proliferation and control of sensitive goods, international sanctions obligations, national security considerations, and considerations concerning the intended end-use and risk of diversion of the goods and/or technology to be exported.

Under the EU regime, exporters are required to keep detailed records of consignments of dual-use goods and technology for at least three years. In addition, exporters who engage in intra-Community trade of controlled dual-use items must provide competent authorities with their names and the addresses where records relating to the transaction can be inspected.

The majority of EU member states do not control the import or use of encryption hardware, software, or technology. However, certain EU legislation, while not restricting the use of encryption, may ultimately have an impact on how encryption goods and technology are used, and on the types of requirements that are placed on providers of encryption-related services. This legislation includes:

1. The Data Protection Directive — The Data Protection Directive⁶ may limit the types of national controls that can be placed on encryption technology. In addition, there may be circumstances in which the Data Protection Directive mandates the use of encryption or digital signature services to ensure the protection of personal information, or implies particular security requirements for the provision of cryptographic services.
2. The Electronic Signatures Directive — The Electronic Signatures Directive⁷ recognizes that divergent member state rules with respect to the legal recognition of electronic signatures and the accreditation of certification service providers may create a significant barrier to the use of electronic communications and electronic commerce within the EU (see text, below).

⁶ Directive 95/46/EC.

⁷ Directive 99/93/EC.

3. The Electronic Commerce Directive — The Electronic Commerce Directive⁸ supports the elimination of national restrictions on the availability and use of encryption technology.

Each of the EU Directives has been implemented by most individual EU member states, and the specifics of the national implementations of the directives can differ (in most cases, in relatively minor respects).

France France has traditionally placed very tight controls on all but the weakest of encryption products. In addition to being a member state of the EU and the Wassenaar Arrangement and regulating exports of encryption accordingly, France has its own system of controls, which include restrictions on not only the import, export, and use of encryption, but also on the “supply” (i.e., sale or distribution to third parties) of encryption products. French encryption controls are administered by the *Direction Centrale de la Sécurité des Systèmes d'Information* (DCSSI), which reports to the Prime Minister through the *Secrétariat Général de la Défense Nationale*.

In June 2004, France passed the Digital Economy Law (*Loi pour la Confiance dans l'économie Numérique*),⁹ becoming the last of the original 15 EU member states to implement the EU Electronic Commerce Directive. The Digital Economy Law liberalizes the supply of encryption products in France, while tightening the rules on the transfer of encryption products outside of France. Among other things, the Digital Economy Law replaces strict authorization requirements for import and use of encryption products with declaration requirements. However, as of February 2005, the implementing Decree for the encryption provisions of the Digital Economy Law had not yet been adopted. It was expected that the Decree would be issued in the summer of 2005.

Czech Republic As a member of the EU and the Wassenaar Arrangement, the Czech Republic regulates the export of encryption products and technology in accordance with EU law and Wassenaar recommendations. However, unlike most EU member states, the Czech Republic also regulates the import of encryption products.

In particular, Act Number 21/1997 (as amended by Act Number 204/2002) and Decrees Number 397/2003 and Number 398/2003 regulate the import of dual-use goods in the Czech Republic. Under these laws, any firm or individual seeking to import a controlled encryption product from a non-EU country to the Czech Republic under a General Import License must first register with the Ministry of Industry and Trade.

8 Directive 2000/31/EC.

9 Law Number 2004-575.

Importers wishing to import very sensitive encryption products are required to obtain an Individual or Individual Open License from the Ministry of Industry and Trade. The Ministry of Industry and Trade will also issue Individual Import Licenses or International Import Certificates when required by officials in the country of origin of a controlled item.

Other States Some other new EU members, such as Latvia, Lithuania, and Slovakia, also tend to have stricter rules than original 15 EU members (except for those of France).

(iv) *China*

Mainland China China regulates the import and export of all hardware and software products “for which their intended functions cannot be fulfilled without implementing encryption or decryption functionality”.

Controlled encryption products require government approval by the State Encoding Control Commission (also known as the State Encryption Management Commission) prior to import or export, pursuant to the Regulations on Commercial Encryption. In addition, the import or export of certain restricted items or technologies requires a license issued by the Ministry of Commerce. Despite several policy clarifications, the approval process to export, import, or use encryption in China remains an extremely *ad hoc* system.

The Regulations on Commercial Encryption do not provide vehicle for distribution of foreign encryption in China. It is illegal for Chinese nationals to use foreign encryption products, although foreign entities or individuals and “foreign-invested enterprises” in China may use foreign encryption for their corporate internal use after registering and obtaining approval from the State Encoding Control Commission.

Hong Kong Hong Kong became a Special Administrative Region (HKSAR) of the People’s Republic of China on 1 July 1997. Despite this reversion to Chinese jurisdiction, Hong Kong remains an independent trading entity and a separate customs territory.

The Basic Law of the HKSAR, which went into effect on the date of Hong Kong’s transfer from British to Chinese control, puts forth the principle of “One Country, Two Systems”, meaning that (for the time being) Hong Kong will retain its capitalist system of government and law. Thus, the Hong Kong Government continues to preside over its own economic and trade matters, including the implementation of export and import controls.

Currently, Hong Kong does not restrict the domestic use of cryptography. However, Wassenaar-like licensing restrictions apply to both export and import of encryption hardware and software under the HKSAR strategic

trade control system. Specifically, the import or export of cryptographic items over 56 bits is regulated by the Trade and Industry Department, unless a license exception (e.g., personal use or mass market exception) applies.

(v) *Russia*

Generally, Russia has the strictest rules in the world regarding encryption. In addition to controls on the import, use, and export of encryption products, the Russian Federation imposes broad controls on the development, distribution, technical maintenance, and manufacture of all encryption products (including hardware, software, and technical materials), as well as the supply of encryption-related services.

Each encryption-related activity requires a license, and there are no significant exceptions from the licensing requirement for particular uses of encryption (e.g., authentication) or particular sectors (e.g., financial institutions). The Federal Security Service has licensing authority for all encryption-related activities. Intangible transfers (e.g., Internet downloads and uploads) of encryption software also are controlled in the country.

(vi) *India*

Pursuant to the Foreign Trade (Development & Regulations) Act of 1992, India uses a so-called “negative list” which sets forth those products whose import and export are controlled. Because encryption items are not currently listed on the “negative list”, their import and export are not explicitly restricted.

However, encryption software could possibly be controlled as a result of the tangible form in which it is transported to India. Although India does not control encryption software stored on CD-ROMs, floppy discs, or magnetic tapes, other storage mechanisms may be subject to licensing requirements. The Department of Telecommunications of the Ministry of Communications and Information Technology controls import of voice encryption products and communications jamming equipment, as well as the export of encryption-based telemetry equipment.

India applies a patchwork of restrictions to the use of encryption. Many uses of encryption (particularly for internal corporate use) are not restricted. However, restrictions could apply to encryption products if used in connection with services interconnected to a public network, or services operated pursuant to an Indian telecoms license. Specifically, there are restrictions under Indian telecommunications law on provision of encryption functionality by certain types of telecommunications service providers.

The standard license (a contract with the government) issued for provision of voice mail and unified messaging services prohibits the licensee from using encryption equipment for bulk encryption of communications. Likewise, the

standard license for Internet Service Providers (ISPs) and the Guidelines for Internet Service issued by the Department of Telecommunications provide that ISPs may use only up to 40-bit encryption (or equivalent level of encryption) as part of the services that they provide.

(vii) Israel

There are import, use, and export licensing restrictions in Israel. Israeli law does not provide exemptions for particular types of encryption products (e.g., encryption products providing authentication functions only) or encryption products of particular key lengths (e.g., products with key lengths less than 56-bits). However, there is a broad exception for the internal use of encryption by a business or an individual.

Under this exception, a license is not required by businesses or individuals for internal or personal use of commercial encryption products acquired in Israel from an entity licensed to sell and distribute them or downloaded from the Internet to be used either for authentication (i.e., to create a digital signature) or to secure information for “self-use” (i.e., internal or personal use). Nevertheless, a license is still required when encryption software is downloaded from the Internet for integration into an encryption product or for encryption development or manufacturing purposes.

Furthermore, imports of encryption items for commercial use (e.g., imports by a retailer for sale and distribution in Israel) continue to require an import license (as well as a license to sell and distribute the encryption items in Israel).

Export controls — although they have been strictly imposed in the past — have been liberalized, and the export licensing process has been streamlined. Under a September 2000 policy, all encryption products are eligible for a restricted license authorizing exports to all non-government end-users in all countries (except for certain countries against which Israel maintains embargoes) after a technical review.

(viii) South Africa

Although South Africa restricts the import and export of encryption products that are destined for a military end-user, it does not presently restrict the export of encryption products that are intended for non-military end-users.

Under the Electronic Communications and Transactions Act 2002, no person is allowed to provide cryptography products or services in South Africa without registering with the Department of Communications.

The Electronic Communications and Transactions Act also establishes a voluntary accreditation scheme for authentication products and services. However, the registration requirement under the Electronic Communications and Transactions Act is currently not in force since the government has

not yet released regulations that set out the detailed requirements for registering encryption products or services, the registration process and costs.

(d) Legal and Regulatory Trends

The general global trend in encryption policies has been one of moderately rapid deregulation of encryption items. As stronger encryption protocols have been developed, governments have continued to ease restrictions on the import, export, and use of products that utilize encryption protocols with lower key lengths.

However, after 11 September 2001, this trend changed to a significant extent. Overall, developed countries (e.g., EU member states and the United States) have continued to relax the regulatory restrictions on encryption products, albeit at a slightly slower pace. In developing countries, however, regulation appears to be increasing.

(e) Policy Issues

Government encryption regulation, as it has been since the advent of encryption regulation, is driven primarily by two distinct, but related, interests, namely:

1. A foreign intelligence interest in collecting all information that implicates national security; and
2. A law enforcement interest in collecting evidence of criminal activity.

The prospect of widely available strong encryption threatens both these interests. The global survey above shows that governments have taken different policy approaches in their efforts to contain the threat they see posed by encryption.

What is the best approach to encryption export, import, and use regulation? Governments can choose between overt domestic regulation, as in China, France, and Russia, and the export-focused policies that now prevail in the domestic markets of the United States and EU.

While countries with advanced encryption industries may have a stronger basis for export controls, other countries that wish to restrict access to information or have aggressive national security structures may have a stronger basis for import/use controls. Certain developing countries might even choose not to control encryption at all if they believe that domestic use of encryption has not become widespread and that they have not had cause to focus on the need for controls. Thus, the answer to the question above may be different for developed countries (particularly those with leading technology and software industries) and developing countries.

However, technological advances and commercial realities have increasingly made strong encryption an essential component of the international infrastructure for electronic commerce. The ability of sophisticated companies and savvy encryption users and developers around the world to sidestep government controls on the export, import, and use of encryption is likely to frustrate the unilateral efforts of individual governments to restrict global availability of strong encryption or to prevent the emergence of secure international communications. While this may call for a new international approach to encryption controls, any international effort without closely coordinated and monitored enforcement is unlikely to succeed.

9.03 Regulation of Electronic Signatures

(a) Types of Electronic Signature Legislation

(i) *In General*

There are several different approaches that have been taken to electronic signature legislation, varying according to the degree of specificity regarding use of particular signature technologies. The legislative schemes can generally be classified as prescriptive, enabling, or hybrid.

(ii) *The Prescriptive Approach*

The earliest electronic signature legislation took the approach of prescribing that particular technology must be used, generally requiring the use of digital signatures based on public key encryption technology.

For example, this approach was taken by the German Digital Signature Law adopted in 1997,¹⁰ and the statutes adopted in the United States states of Utah in 1995¹¹ and Washington in 1997.¹²

The prescriptive approach has the significant disadvantage that it eliminates flexibility regarding implementation of electronic signature technology. In the fast-changing e-commerce technology environment, such a lack of flexibility is usually commercially unacceptable. As a result, the prescriptive approach to electronic signatures has largely been abandoned.

(iii) *The Enabling Approach*

Under the enabling approach, all electronic signatures are potentially valid. That is, a signature may not be denied effect solely because it is in electronic form — although in certain cases there are exceptions for particular types of

10 *Informations-und Kommunikationsdienste-Gesetz*, BT-Drs. 13/7934, 11 June 1997.

11 Utah Digital Signature Act, Utah Code, section 46.

12 Washington Electronic Authentication Act, R.C.W. 19.34.

transaction that must be “on paper” (e.g., real property or notarial transactions). The weight that is attached to a particular electronic signature under the enabling approach is an evidentiary issue to be decided in court (to the extent a signature is challenged).

For example, the writing of the author’s name in an email (or even the mere sending of an email) could be construed as a valid electronic signature. If such a signature were challenged, the recipient or other party asserting the validity of the signature would need to prove facts sufficient to establish its validity, such as facts relating to the computer systems over which the email was sent and received.

The enabling approach is the one that has been taken in the United States, including in the Uniform Electronic Transactions Act (a model law which has now been adopted by almost all United States states) and the federal Electronic Signatures in Global and National Commerce Act. These statutes are discussed in further detail below.

The enabling approach has the significant advantage of placing no barriers on development of technology. Some signature technologies may succeed in the market because they provide heightened indicia of reliability, while others may succeed because of ease of use. Furthermore, the requirement to prove signature validity is a familiar issue for courts and has arisen often in the context of handwritten signatures.

(iv) The Hybrid Approach

The hybrid approach combines the enabling and prescriptive approaches, seeking to realize the benefits of both. It incorporates the enabling approach, but also provides that electronic signatures using particular technologies are entitled to a special presumption of validity. For example, this is the approach taken by the EU Electronic Signatures Directive¹³ (see text, below).

The hybrid approach has most of the advantages of the enabling approach, but does provide technological guideposts for high-reliability digital signatures. The latter feature of the hybrid approach has both advantages and disadvantages. On the one hand, it identifies signatures that will be deemed valid with significantly reduced requirements of evidentiary proof in court. On the other hand, it suffers a disadvantage analogous to the prescriptive approach, i.e., that it confines development of technologies for high-reliability digital signatures.

(b) Global Survey of Regulation

(i) European Union

The EU Electronic Signatures Directive recognizes that divergent member state rules with respect to the legal recognition of electronic signatures and

13 Directive 1999/93/EC.

the accreditation of Certification Service Providers (CSPs) may create a significant barrier to the use of electronic communications and electronic commerce within the EU.

Aimed at creating a “clear Community framework regarding conditions applying to electronic commerce [in order to] strengthen confidence in, and general acceptance of, the new technologies”, the Electronic Signatures Directive provides for the legal recognition of electronic signatures and the establishment of national CSP accreditation schemes.

The Electronic Signatures Directive adopts the hybrid approach to electronic signature legislation. It does not set particular requirements for the legal recognition of electronic signatures.¹⁴ Under the Electronic Signatures Directive, no electronic signature may be denied legal effectiveness or admissibility in legal proceedings solely on the grounds that it is in electronic form.¹⁵

However, “advanced electronic signatures”,¹⁶ based on “qualified certificates” and created by a “secure-signature-creation device”, will receive heightened evidentiary consideration (and are deemed the legal equivalent of hand-written signatures).¹⁷ The Electronic Signatures Directive’s three Annexes set the requirements for qualified certificates, Certification Service Providers issuing qualified certificates, and secure-signature-creation devices.

The Electronic Signatures Directive also takes other steps to eliminate obstacles to the establishment of a single “electronic” market. It prohibits mandatory CSP accreditation schemes and the discriminatory treatment of CSPs based in other member states, and it sets standards for the recognition of qualified certificates issued by CSPs in third countries.¹⁸ It also sets minimum liability standards for CSPs that issue qualified certificates or guarantee their certificates to the public and reaffirms the obligation of CSPs to comply with the EU requirements concerning the transfer of personal data.¹⁹

(ii) *United States*

As mentioned above, the enabling approach has been adopted by both the Uniform Electronic Transactions Act of 1999 and the federal Electronic Signatures in Global and National Commerce Act of 2000 (E-SIGN Act),²⁰ these

14 Electronic signatures are defined in article 2(1) of the Directive as “data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”.

15 Electronic Signatures Directive, article 5(2).

16 Electronic Signatures Directive, article 2(2).

17 Electronic Signatures Directive, article 5(1).

18 Electronic Signatures Directive, articles 3, 4, and 7.

19 Electronic Signatures Directive, article 8(1).

20 15 United States Code, sections 7001 *et seq.*

having adopted a minimalist approach to enabling the use and recognition of electronic signatures without mandating use of specified technology (e.g., the operation of public key infrastructures).

The Uniform Electronic Transactions Act is technologically-neutral model legislation that gives legal effect to electronic signatures, contracts, and other transactional records. The Uniform Electronic Transactions Act does not require any particular technology to be used for an electronic signature, and allows parties to prove the validity of an electronic signature by demonstrating that it was “executed or adopted by a person with the intent to sign the electronic record”.

Under the Uniform Electronic Transactions Act, an electronic signature can be proven “in any manner” to be attributed to a particular person, including by reference to the security procedure used to create the signature. The effect of an electronic signature attributed to a particular person is to be determined from the “context and surrounding circumstances at the time of its creation”, including any agreement that the parties have entered into concerning the use of electronic signatures.

As of January 2005, 46 states, the District of Columbia, and the United States Virgin Islands had adopted the Uniform Electronic Transactions Act. The E-Sign Act has similar effect in the few United States states that have not yet adopted the Uniform Electronic Transactions Act.

(iii) Canada

The federal Personal Information Protection and Electronic Documents Act defines an “electronic signature” as:

... a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document.

The Personal Information Protection and Electronic Documents Act provides that legal signature requirements under certain listed federal legislation are satisfied if the regulations have been complied with. However, certain types of electronic documents (e.g., sworn statements, witnessed documents, originals, and sealed documents) require a “secure electronic signature”, defined in the Personal Information Protection and Electronic Documents Act as an “electronic signature that results from the application of a technology or process prescribed by regulations”.

In February 2005, the Canadian government issued the Secure Electronic Signature Regulations pursuant to the Personal Information Protection and Electronic Documents Act and the Canada Evidence Act. The Secure Electronic Signature Regulations require the use of digital signatures created using public key encryption and specify that a secure electronic signature is

trustworthy only if it is created using a “digital signature certificate” issued by a reliable certification authority (i.e., an authorized certification authority that has been verified by the President of the Treasury Board of Canada as having the capacity to issue digital signature certificates in a secure and reliable manner).

In addition, the Secure Electronic Signature Regulations provide that an electronic document signed with a digital signature for which a certificate was issued by an authorized certification authority would carry a rebuttable presumption that the electronic document is attributable to the person identified by the digital signature certificate.

(iv) Singapore

Under section 8 of the Singapore Electronic Transactions Act 1998, secure electronic signatures are given full legal effect as a signature. The Singapore Electronic Transactions Act is based largely on the Model Law on Electronic Commerce issued by the United Nations Commission on International Trade Law (UNCITRAL) and certain United States legislation.

According to the Singapore Electronic Transactions Act, any letters, characters, numbers, or other symbols in digital form used by a person with the intention of authenticating an electronic record can constitute an “electronic signature”.

Recognizing that electronic signatures may be easily forged, the Singapore Electronic Transactions Act provides that a “secure electronic signature” is an electronic signature that can be verified, by a secure procedure prescribed by the Singapore Electronic Transactions Act (i.e., the use of digital signatures and public key encryption) or commercially reasonable security procedure agreed by the parties involved, to be:

1. Unique to the signatory;
2. Capable of identifying such a person as the signatory;
3. Created in a manner or using a means under the sole control of the person using it; and
4. Linked to the associated electronic record so that any tampering with such record can be detected.

Specific legal presumptions apply to a secure electronic signature — it is presumed that it is the signature of the signatory and that the signatory intended to maintain the authenticity and integrity of the electronic record signed with a secure electronic signature. This would prevent the signatory from easily repudiating a validly signed electronic document. With a non-secure ordinary electronic signature, no such legal presumptions can be made.

(v) South Africa

Under the Electronic Communications and Transactions Act, which came into effect on 2 August 2002, no person is allowed to provide cryptography products or services in South Africa without registering with the Department of Communications. The Electronic Communications and Transactions Act also establishes a voluntary accreditation scheme for authentication products and services.

The South African Accreditation Authority established under the Electronic Communications and Transactions Act has the responsibility for assessing applications and accrediting certain electronic signatures as “advanced electronic signatures”.

The Department of Communications issued draft Accreditation Authority Regulations and Cryptography Regulations for public consultation in July and September 2004, respectively. The proposed Cryptography Regulations contain detailed requirements for registering encryption products or services, the registration process, and costs. However, the registration requirement under the Electronic Communications and Transactions Act has yet to be fully implemented since the government had not yet released finalized Cryptography Regulations.

(vi) Thailand

The UNCITRAL Model Law on Electronic Commerce (1996) and the UNCITRAL Model Law on Electronic Signatures (2001) were used as guidelines in drafting Thailand’s Electronic Transactions Act. Under the Thailand Electronic Transactions Act, which came into effect in April 2002, an electronic signature constitutes a valid and binding legal signature in Thailand.

The Thailand Electronic Transactions Act defines “electronic signature” in a similar way to Singapore’s Singapore Electronic Transactions Act. The Thailand Electronic Transactions Act also specifically provides that any data or record may not be denied legal effect and enforceability solely because it is in electronic form. This is to ensure that Thailand has an effective legal framework to successfully enforce electronic contracts and to allow the courts to accept evidence in the form of electronic documents.

(vii) Ukraine

The Law of Ukraine on Electronic Digital Signature came into effect on 1 January 2004. While the Law gives legal effect to electronic signatures (so that they are equivalent to handwritten signatures and corporate seals that are commonly used in Ukraine), a related Law of Ukraine on Electronic Documents and Electronic Circulation of Documents provides legal effect to documents in electronic commerce environment.

The Ministry of Transport and Communications of Ukraine was assigned the role of a “centralized” certification authority with responsibility to issue digital certificates and accredit entities involved in the certification of digital signatures, pursuant to the Cabinet of Ministers of Ukraine Resolution Number 1451 on Approving the Regulations of the Central Certifying Body of 28 October 2004.

(viii) United Nations Commission on International Trade Law

In July 2001, UNCITRAL adopted the Model Law on Electronic Signatures (the “2001 Model Law”). The 2001 Model Law was designed to assist national legislatures in developing a modernized, harmonized, and fair legislative framework to facilitate the use of electronic signatures. By encouraging nations around the world to adopt the 2001 Model Law, UNCITRAL hoped to foster economy and efficiency in international trade.

Created as an extension of the UNCITRAL Model Law on Electronic Commerce (1996), the 2001 Model Law offers practical standards against which the technical reliability of electronic signatures may be measured, and it does not favor the use of any particular technology. Specifically, the Model Law states that an electronic signature is considered “reliable” if it is:

1. Uniquely linked to the signatory;
2. Created in a manner that is under the sole control of the person using it;
3. Incapable of being altered without detection; and
4. Linked, when required by law, to the associated electronic record so that any alteration to the record can be detected.

In addition to these criteria, the Model Law establishes basic rules of conduct that are to be observed by the various parties involved in the electronic signature process (including the signatory, the relying party, and any trusted third party).

(c) Public Key Infrastructure

“Public key infrastructure” (PKI) refers to rules, technologies, and physical infrastructure that allow digital signature and encryption use public key encryption technology. Because PKI offers the possibility for digital signatures to be used broadly by a large group of individuals, it offers major potential benefits for electronic commerce and electronic government.

However, these benefits have been widely advertised for roughly a decade, with fairly limited achievements in practice — as a result of limitations and risks of PKI technologies that have become increasingly apparent. Nevertheless, in the last few years PKI has seen substantial growth in controlled environments.

PKI essentially provides a means in which the “public keys” used to verify digital signatures of particular individuals (or to send encrypted messages to those individuals) are widely available on the Internet or another network. The technological details of how this works are beyond the scope of this chapter. However, it is possible to identify three general legal and procedural requirements for an effective PKI.

First, there must be legal recognition of digital signatures performed using PKI. This requirement is fulfilled by the electronic signature laws discussed above. Second, there must be a trusted party — often called a Certification Authority (CA) or Certification Service Provider (CSP) — that issues and verifies public keys. Third, there must be defined procedures regarding how signing parties use their keys and how relying parties may rely on such signatures.

It is not too difficult to develop software, hardware, and procedures that theoretically satisfy these requirements. However, the devil, as it is often said, is in the details. A number of significant practical difficulties have emerged in deployment of PKIs:

1. Certification Authority liability — It is necessary to specify the extent to which a CA bears liability for improperly issuing a certificate. Many prospective CAs are unwilling to bear sufficient liability to make their certificates appropriate for use in high-value transactions.
2. Standards and interoperability — Because of the high degree of specificity of PKI implementations, there have been significant difficulties in ensuring interoperability of electronic signatures, even among users implementing the same technology. A particular problem in this area is that available PKI standards are insufficiently precise. For example, the leading x.509 v3 for digital certificates, developed by the International Telecommunication Union (ITU), allows for significant variation among certificates.
3. Certificate revocation — To ensure that a particular certificate is valid, it is typically necessary to check the “certificate revocation lists” of the CA that issued the certificates. Effective means to do so in the context of a public PKI have developed slowly.
4. Security — There are numerous security risks associated with PKIs. These include the possibility that individual users fail to secure their “private keys” that are used in the signature process, and the possibility that the facilities of a CA or other signature infrastructure could be compromised. These security risks are related to the risks of CA liability and certificate revocation.

The combined effect of these risks is that there has been extremely slow development of broadly available public PKIs. These have been successful only in narrow applications.

For example, Secure Sockets Layer (SSL) certificates are widely deployed to identify web sites for secure transactions. This application only requires that the certificate associate a particular public key with the web site that a user has accessed. In this application, many of the issues noted above are significantly reduced.

VeriSign and a few other companies sell low-cost certificates via the Internet, which offer minimal liability protection and which are generally suitable only for low-value transactions or transactions with entities or individuals that are independently trusted.

With respect to use of PKIs in higher-risk situations, the trend is for development of purpose-specific “private” PKIs, rather than widely interoperable PKIs. For example, PKI technology is beginning to be widely used by banking networks, and various multinational companies are deploying PKIs to support their global operations. A few countries (generally not including large industrialized economies) have also explored use of PKI as the basis for national identification systems (e.g., on PKI-based identity cards).

(d) Policy Issues

What is the best approach to electronic signature regulation? Of the general approaches to electronic signature regulation described above, the prescriptive approach has clearly been discredited. Between the enabling and hybrid approaches, these authors believe there are arguments on both sides. Although the hybrid approach is now the majority view (outside the United States), the risk of constraining development of high-security electronic signatures is in our view significant.

In the EU, where the hybrid approach has been adopted by the Electronic Signatures Directive, few entities have chosen to implement advanced electronic signatures. However, this may change if EU governments and other entities begin to require that advanced electronic signatures be used to perform particular types of transactions and interactions — and the hybrid approach does offer the benefit of a degree of standardization for high-security signatures used in such circumstances. In addition, in any event, the hybrid approach is likely to remain the legal reality in the EU, Canada, and elsewhere.

As noted above, an absolute prerequisite to promoting use of electronic signatures and PKI is the passage of law ensuring the validity of electronic signatures. This has already occurred in most of the developed world, and significant parts of the developing world.

Beyond this, these authors believe that development of electronic signatures and PKI should be largely left to the market. Thus, entities considering the

use of electronic signatures in particular applications, including governments considering their use for e-government applications, should assess the benefits and costs of the particular use, considering issues including the risk factors that are addressed above. Over time, it appears likely that use of electronic signatures and deployment of PKI will increase, including because techniques will gradually be developed to deal with the above risk factors.

It is certain that the near- and medium-term potential for PKI has periodically been exaggerated by those with an interest in promoting its development. In large part, proponents of PKI have under-weighted risk factors like those noted above. However, in the longer term, benefits of PKI will certainly outweigh risks in a variety of applications. As discussed above, this is already occurring fairly broadly in corporate and other “closed” PKI applications.

