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

OLIS : 04-Oct-1999
Dist. : 05-Oct-1999

Or. Eng.

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

Working Party on Information Security and Privacy

INVENTORY OF APPROACHES TO AUTHENTICATION AND CERTIFICATION IN A GLOBAL NETWORKED SOCIETY

82311

CONTEXT FOR THE INVENTORY

Snap-Shot View

This report has been prepared by the Working Party on Information Security and Privacy based on input supplied by Member countries. It represents a "snap-shot" view of OECD Member country approaches to authentication and certification on global networks, including information about laws, policies and initiatives, in both the public and private sectors and at the national, regional and international levels, as reported by Member countries as of *July 1999*. It is important to note that in many Member countries these approaches are still being developed, in light of evolving technologies, and in consideration of work underway at the European Union and international level. This inventory should be considered a work-in-progress report that represents the ongoing information exchange among the members of the Working Party.

Private Sector Role

The Group of Experts recognises the leading role of the private sector in the development and use of authentication and certification technologies and mechanisms in the electronic environment. Technologies and business models for authentication and certification are continuing to develop on a global scale, and the private sector has begun to outline frameworks and develop model systems for specific technology applications. The rapid pace of technological evolution and the diverse models for authentication and certification that are currently emerging in Member countries make it difficult to adequately survey the private sector activities in this area. Therefore, this inventory does not include a separate chapter focusing on private sector initiatives. However, where countries have reported on the activities of their private sector actors, this has been included as part of the national approach section. The proceedings of the Joint OECD-Private Sector Workshop on Electronic Authentication contain significant information about private sector initiatives in this area.

INVENTORY OF APPROACHES TO AUTHENTICATION AND CERTIFICATION IN A GLOBAL NETWORKED SOCIETY

OVERVIEW

Authentication is used in the electronic environment to establish identity or privileges, or as part of payment mechanisms, for instance through the use of a password or smart card, or by using a cryptographic, shared secret or biometric technique. Certification mechanisms can provide assurances about information in the electronic environment to reduce uncertainty in electronic transactions between parties or systems. For instance, a trusted source could attest to some fact to provide a way to determine that the information is verifiably connected to a transacting party. Where authentication relies on cryptography technologies, a certification mechanism could be used to link the public cryptographic key with an individual or entity. A wide variety of technologies and mechanisms are available to authenticate and certify various elements of electronic transactions, and a number of different architectural models are under consideration in OECD countries.

As OECD countries turn their attention to developing policies and laws to facilitate electronic commerce, they are looking at issues related to authentication and certification in a global networked society. Conflicting national solutions for electronic authentication and certification could have an impact on the development of global electronic commerce. The OECD plays a role in this area by providing a venue for ongoing information exchange in order to clarify the issues related to authentication and certification and provide a solid basis for ongoing international co-operation in this area. The ICCP Committee's Working Party on Information Security and Privacy continues the dialogue involving governments, business and industry, and user representatives to examine more fully the technologies and diverse models for authentication and certification to facilitate global electronic commerce which are currently in use or emerging in Member countries. This *Inventory of Approaches to Authentication and Certification in a Global Networked Society* continues the survey of activities in OECD countries related to authentication and certification on global networks, including information about laws, policies and initiatives in the public and private sectors, and at the national, regional and international levels. Specifically, the report looks at:

- Private contractual agreements
- Technology requirements
- Standards, and
- Certification authorities.

TABLE OF CONTENTS

QUESTIONS FOR FRAMING INPUT TO THE REVISED INVENTORY

The following questions have been identified by Member countries to assist Delegations in framing their written input to the inventory. For the purposes of this inventory, "digital signature" means electronic authentication based on public key cryptography, and "electronic signature" means any signature in electronic form.

General

Following upon the October 1998 *Ministerial Declaration on Authentication for Electronic Commerce*, has your country taken any steps to amend, where appropriate, technology or media specific requirements in current laws or policies that may impede the use of information and communication technologies and electronic authentication mechanisms, giving favourable consideration to the relevant provisions of the 1996 UNCITRAL Model Law on Electronic Commerce? If yes, please describe.

1. Does your country have a specific law or regulation concerning digital signatures, electronic signatures, or other kinds of electronic authentication? If yes, please give reference information.
2. In the absence of a relevant law, regulation or standard, does your country recognise at the national or sub-national level any published criteria, the observance of which render electronic documents or signatures admissible for evidentiary purposes? If yes, please give reference information.
3. Is there a public or private sector body in your country that issues digital certificates for public use? If yes, please describe.
4. Does your country use authentication technologies or mechanisms in the electronic delivery of government services to citizens? If yes, please describe.
5. Are there any initiatives, studies, proposed legislation or rules, or other activities currently underway or under consideration -- in the public or private sectors -- in the area of authentication and certification in your country? If yes, please describe.
6. Are there private sector models for electronic authentication that are in operation or under development in your country? If yes, please describe.
7. Please provide, where possible, contact points at the national level where readers of the inventory report could direct follow up questions.

Private contractual agreements

8. What is the effect of your country's law or regulation on private contractual agreements concerning the use and recognition of digital signatures, electronic signatures, or other kinds of electronic authentication?

9. Are parties free to agree to standards, procedures, and uses that differ from those set forth in national laws and regulations?

10. If they enter into an agreement that sets standards, procedures, or uses that differ from those set forth in national laws and regulations, may the parties use the national legal system to attempt to attain redress under the terms of the contract?

11. Do any evidentiary standards apply to evidence of validity and authenticity offered to a judicial or administrative proceeding in your country? If so, what methods of proof are available?

Technology requirements

If you answered "yes" to Number 2, above:

12. Does your country's law or regulation specifically approve a particular kind of electronic authentication technology or mechanism? If so, what is the effect of your country's laws or regulations on the use of an electronic authentication mechanism that is not specifically approved? Do your country's laws or regulations preclude or disadvantage a party using an authentication method other than one specifically approved?

13. Are parties using electronic authentication methods other than one specifically approved by law or regulation able to establish the validity and authenticity of that method by offering evidence of its reliability in a judicial or administrative proceeding? If so, is the access to judicial or administrative proceedings predicated on any requirement of local partnership or establishment of one of the parties?

14. Does your country's law or regulation identify certain electronic authentication technology as "secure"? If so, please describe.

15. Does your country's law or regulation differentiate between levels of security? If so, how? What are the legal consequences of this distinction?

16. Does your country's law or regulation set forth technical requirements for components or systems for electronic authentication? If so, how are these technical requirements determined? Are the requirements mandatory, or are they provided only as guidance?

17. Does your country's law or regulation require that technical components or systems used in electronic authentication be accredited or licensed? If so, please describe the mechanisms for accreditation or licensing, including the private sector role.

18. What are the consequences in a judicial or administrative proceeding, of using an alternative to the legislatively- or administratively-approved method of electronic authentication?

Standards

19. Have any national or sub-national standards for electronic authentication been developed by the public or private sectors in your country? If yes, please describe.

20. Are there laws, regulations or private sector mechanisms governing or developing/setting standards for digital signatures, electronic signatures, or other kinds of electronic authentication in your country? If yes, please describe.
21. Is compliance with any standards mandatory in your country? If yes, please provide reference information for mandatory standards.
22. Could the failure to follow your country's standards give rise to liability in civil proceedings, or increase the likelihood that a party will be held liable for the use of an alternative standard? If yes, please describe.
23. Does the private sector play a role in developing and certifying standards for digital signatures, electronic signatures, or other kinds of electronic authentication in your country? If yes, please describe.
24. Do your country's laws and regulations permit private-sector bodies to certify compliance with legislatively- or administratively-approved standards? If yes, please describe.
25. Please identify private sector initiatives in your country concerning standards and related issues in the area of authentication.

Certification authorities

26. Are any measures being taken to evaluate and approve, or accredit, certification authorities (or other providers of trusted services) in your country? If so, please describe.
27. Do your country's laws or regulations govern or set requirements for licensing or accrediting "certification authorities" (or other providers of trusted services)? Are there private sector models for accreditation of certification authorities that are in operation or under development in your country? If so, what requirements must a certification authority meet? Do the laws or regulations have mechanisms to recognise private sector-accredited entities? Do the requirements vary by sub-national jurisdiction?
28. What liability rules currently apply to the activities of certification authorities in your country? Are there any proposals to limit the liability of certification authorities in your country? If so, please describe?

Global authentication

29. Do your country's laws or regulations recognise digital signatures, electronic signatures, or other kinds of electronic authentication used in other countries? If yes, please describe.
30. To the extent that there are laws or regulations concerning providers of trusted services related to digital signatures, electronic signatures, or other kinds of electronic authentication in your country, are there procedures to recognise foreign providers of similar services? If yes, please describe.
31. Do your country's laws or regulations place limitations on cross-border recognition of electronic authentication? If yes, please describe.

32. Is there a central public or private sector body that will cross-certify certification authorities at the national or sub-national level in your country? If yes, do cross-certification procedures vary by sub-national jurisdiction?

33. Are there any private sector models in your country for cross-certification of certification authorities? If yes, please describe.

34. Do your country's laws or regulations place limitations on cross-certification between certification authorities operating in your country and certification authorities in other countries? If yes, please describe.

NATIONAL APPROACHES

Australia

Authentication -- Legal and policy initiatives and the Australian approach

In March 1998 the Australian Attorney-General's Electronic Commerce Expert Group issued the report "Electronic Commerce - Building the Legal Framework"[1]. The Attorney-General announced that legal obstacles to the development of electronic commerce will be removed by uniform legislation to be developed in consultation with the State and Territory governments. The proposed legislation will be based on the Report, which recommended that legislation should be based on the UNCITRAL Model Law on Electronic Commerce. The Australian Government released the report "Gatekeeper - A strategy for public key technology use in government"[2] in May 1998 as part of its "Government Online" initiative. The Australian Government has now established a Government Public Key Authority to implement Gatekeeper[3]. The Victorian Government issued the discussion paper "Promoting Electronic Business: Electronic Commerce Framework Bill"[4]. The Standards Australia[5] subcommittee on public key authentication issued two draft standards as part of a series of standards to implement the Standards Australia report "Strategies for a Public Key Authentication Framework in Australia" (MP75/96). The Australian Government established a National Public Key Infrastructure Task Force to examine the implementation of the Standards Australia Report. The Task Force report is expected to be released soon, and will be posted to the National Office for the Information Economy Website.[6]

Certification

As the Australian approach focuses on technology neutrality, the proposed law will recognise all forms of electronic authentication, including public key infrastructures and certificates issued within them. The technical standards and policy frameworks will support public key infrastructure without precluding the use of other electronic authentication techniques where appropriate.

---

1. *Electronic Commerce: Building the Legal Framework*, Electronic Commerce Expert Group to the Attorney General, Australia, 31 March 1998. See http://law.gov.au/aghome/advisory/eceg/ecegreport.html.

2. *Gatekeeper, A Strategy for Public Key Technology Use in the Government*, Office of Government Information Technology, Australia, May 1998. See http://www.ogit.gov.au/gatekeeper/index.html.

3. See http://www.gpka.gov.au.

4. See http://www.mmv.vic.gov.au.

5. See http://www.standards.com.au.

6. See http://www.noie.gov.au.

Authentication, certification and related services

The proposed law will support electronic transactions in all sectors. The media neutrality approach will ensure that there is no difference in Australian law between paper and electronic transactions.

International aspects

Australia supports a three-tiered international approach to continuing work in this area: UNCITRAL for legal issues; OECD, and APEC for government policy framework; and national and international standards making bodies for technical standards.

National contact point

- In addition to the Website URLs included in the footnotes for the resources mentioned above, further information can be requested from crypto@ag.gov.au.

General

Following upon the October 1998 *Ministerial Declaration on Authentication for Electronic Commerce*, Australia has developed the draft Electronic Transactions Bill that adopts a number of provisions of the 1996 UNCITRAL Model Law on Electronic Commerce. Once enacted, this Bill will set in place a light-handed regulatory framework that will facilitate the development of electronic commerce. Australia has adopted a generic principled approach to signatures. This is demonstrated by clause 10 of the draft Electronic Transactions Bill that adopts Article 7 of the UNCITRAL Model Law. The proposed legislation is an interpretation-style law. It will form the blueprint for a national uniform legislative scheme to remove legal impediments to electronic commerce. For further information see http://www.law.gov.au/ecommerce. Clause 10 of the proposed Electronic Transactions Bill concerns electronic authentication, it adopts Article 7 of the UNCITRAL Model Law. See http://www.law.gov.au/ecommerce. Australia does not recognise at the national or sub-national level any published criteria, the observance of which render electronic documents or signatures admissible for evidentiary purposes. Examples of public or private sector bodies that issue digital certificates are KeyPost (http://www.auspost.com.au/keypost), the KPMG Certification Authority (http://www.kpmg.com.au), Baltimore Technologies Asia Pacific (http://www.zergo.com/) and Spyrus (http://www.spyrus.com.au). As recommended by Project Gatekeeper (http://www.ogo.gov.au/gatekeeper), the Government Public Key Authority will provide an authentication framework using public key technology for dealings with the Commonwealth government.

Although Australia does not, as yet, use authentication technologies or mechanisms in the electronic delivery of government services to citizens, there are a number of projects underway that will allow this to happen in the near future. For example: the draft Electronic Transactions Bill will facilitate electronic service delivery by government, and Project Gatekeeper will provide an authentication framework for dealings with the Commonwealth government. Two examples of Commonwealth pilot implementations are the Australian Taxation Office (ATO) and the Australian Securities and Investments Commission (ASIC). ATO held a trial of submitting individual taxation returns via the Internet. Individuals used their tax file numbers as the authentication mechanism and downloaded necessary software from the ATO Internet site. ASIC commenced its Electronic Company Registration (ECR) production pilot on 26

October 1998 with the first electronic registration of an Australian company. The ECR system allows ASIC clients to electronically prepare applications for registration, digitally sign them using private keys stored on cryptographic smart cards and transmit them to ASIC over the Internet. Australia Post's KeyPOST provides the registration and certification authority functions. See: http://www.asic.gov.au.

There are many initiatives, studies, proposed legislation or rules, or other activities underway or under consideration in the public or private sectors in the area of authentication and certification.

- On 6 May 1998, the Minister for Finance and Administration officially launched GATEKEEPER: *A strategy for public key technology use in the Government*. GATEKEEPER was developed by the Office for Government Online in response to the identified needs of agencies to introduce public key technology to support authentication and identification in Government online transactions. The strategy ensures that this is done under a whole of government framework that ensures interoperability, integrity, authenticity and trust for both agencies and their customers.

- Accreditation criteria for certification authorities were released in December 1998 (http://www.gpka.gov.au).

- An evaluator 'panel' of Commonwealth agencies has been established to provide evaluations against Government Public Key Authority (GPKA) criteria. This panel will be expanded over time to include private sector organisations.

- A commercial certification authority service provider is currently under evaluation by the GPKA. Accreditation should be granted in early 1999.

- A Whole of Government Head Agreement for certification authority services is under development.

- OGO is a founding member of the Certification Forum of Australia, the new certification authority industry forum.

- Standards Australia has issued components of the Australian draft PKAF standards for public comment. See: http://www.ogit.gov.au/gatekeeper/index.html; http://www.gpka.gov.au, http://secure.standards.com.au/Catalogue/Script/Search.asp and enter PKAF.

There are also numerous private sector models for electronic authentication that are in operation or under development. The Australian Payments Clearing Association (APCA) is a public company owned by the banks, building societies and credit unions. It has been in existence since February 1992 and has specific accountability for key parts of the Australian payments system, particularly payments clearing operations. APCA announced some time ago that it was developing a framework to support its members' participation in electronic commerce. The framework will encompass a body of policies and rules governing the issuance of digital certificates from APCA to its members and, in turn, from its members to their customers. The provision of digital certificates to its members will become a new corporate function of APCA. A tender process has recently been completed to select a vendor to produce certificates on APCA's behalf. The outcome is that Baltimore Pty Ltd (previously Zergo Asia Pacific) has been selected as the preferred vendor subject to successful progression through a number of checkpoints. See: http://www.apca.com.au/.

Private contractual agreements

The draft Electronic Transactions Bill (and relevant mirror legislation under the uniform national legislative scheme) will allow electronic authentication to meet existing legal requirements for signatures. Parties to private contractual agreements may choose the appropriate form of authentication technology and implementation model for the transaction. To the maximum extent possible, those technologies and implementation models will be recognised and enforced. In that respect, the authentication technology must meet the minimum standards in the draft Electronic Transactions Bill in order to meet any existing legal requirements. Parties may agree to different rules from those set out in the draft Electronic Transactions Bill in relation to the time and place of dispatch and receipt of electronic communications and the attribution of electronic communications. Parties to private contractual agreements may choose the appropriate form of authentication technology and implementation model for the transaction. To the maximum extent possible, those technologies and implementation models will be recognised and enforced. If parties enter into an agreement that sets standards, procedures, or uses that differ from those set forth in national laws and regulations, they may use the national legal system to attempt to attain redress under the terms of the contract.

Standards

Standards Australia, through various working groups has developed or is currently developing standards relating to public key authentication, biometrics and the protection of PINS and passwords in electronic debit transactions. Membership of Standards Australia working groups is open to anyone. Members participate on a voluntary basis, donating their time and expertise free of charge. Working group IT12/4/1 is comprised mainly of private sector representatives. Whilst compliance with some standards are mandated through legislative reference this does not apply in the field of electronic commerce or electronic authentication. Australian private-sector bodies are permitted by national law and regulation to certify compliance with legislatively - or administratively-approved standards but not in the fields of electronic commerce or electronic authentication. There are many private sector initiatives in Australia concerning standards and related issues in the area of authentication. Among other initiatives, the private sector has established a Certification Forum of Australia http://www.aeema.asn.au/_private/frames/frbulletin2.htm).

Certification authorities

Prominent industry associations are pursuing the establishment of a standards-based framework whereby certification authorities (products and services) could be certified as complying with relevant standards by organisations that have been accredited to undertake the certifying function. These certifying organisations would be accredited by the Joint Accreditation System for Australia and New Zealand (JAS-ANZ) under ISO/IEC Guide 62 or 65. The relevant standards against which certification authorities would be evaluated for compliance would include, but may not be limited to, those discussed above. There are no legislative requirements in Australia for licensing or accrediting certification authorities or to recognise private sector accreditation. There are some private sector initiatives for accreditation or certification by the private sector and a government internal scheme involving accreditation. Normal commercial liability rules apply to the activities of certification authorities in Australia. There are no proposals to limit liability other than through contract.

Global authentication

Australia's laws recognise digital signatures, electronic signatures, or other kinds of electronic authentication used in other countries. The draft Electronic Transactions Bill sets out a generic principled approach to signatures based upon Article 7 of the UNCITRAL Model Law. Electronic authentication methods used in other countries could be legally recognised in Australia if they met the tests set out in the Electronic Transactions Bill. Australia's laws and regulations do not place limitations on cross-border recognition of electronic authentication. However, there is no certification authority that will cross-certify at the national or sub-national level, and no private sector models for cross-certification of certification authorities.

National Contact Points

- crypto@ag.gov.au

Austria

A law on digital signatures exists (Signaturgesetz, Federal Law Bulletin I Nr. 190/1999) and will enter into force on 1 January 2000 (sec. 27). The ordinance specifying the technical requirements such as key length is being prepared. The German text of the Law can be downloaded from http://www.ris.bka.gv.at.

General

There are many initiatives, studies, proposed legislations, rules and other activities currently underway or under consideration in the public or private sectors in the area of authentication and certification in Austria. The following list is by no means complete:

- The ARGE Daten offers certification services (https://keyserver.ad.or.at/adcert/).
- The STUZZA (Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr) is involved in a Pilot project.
- The Datakom Austria GmbH. (http://www.datakom.at/) offers several E-Commerce solutions based on EDIFACT and is involved in pilot projects.
- A-Sign is running a demo service that will turn in to a full CA (http://www.a-sign.at/).
- E-Sign is another contender (http://www.e-sign.at/). Their service is scheduled to commence in summer 2000.
- The IAIK (Institute for Applied Information Processing and Communications), an Institute of the Graz University of Technology is heavily involved in electronic signature projects. However, their Web page is under construction (http://www.iaik.tu-graz.ac.at/Research/PKI/index.html).

It can be expected that 3-5 Certification businesses will open in 2000, and perhaps a dozen are expected to be active by 2005.

Private parties may enter into any agreement they see fit, as long as it is not contrary to law.
Austrian law does not forbid parties to agree to a specific form of contract.

A secure signature is equal to a regular signature on paper according to sec. 4 of the Signaturgesetz, and a digitally signed file will be equal to a signed document. There are exceptions for family law (meaning one cannot marry by digital signature) and declarations of surety (declarations of surety should be considered carefully), as well as exceptions for agreements requiring a public notary or an entry into a public register.

So far, the banking industry has shown great interest in digital signatures to promote telebanking. There are cautious plans to facilitate interaction between citizens and governmental agencies by digital signature. A homepage that contains information about legal requirements and possibilities is already online (http://www.help.gv.at) and may develop into a platform for electronic interaction, dubbed "virtual administration".

Standards

As yet, no national or sub-national standards for electronic authentication have been developed by the public or private sectors in Austria.

Certification authorities

Anybody can open a certification authority, in accordance with the planned EG directive. The supervisory authority shall have the right to supervise the certification authorities. Note that only secure Certificates - which require a high level of legal and technical reliability - are equal to the traditonal signature, which means that only CA's issuing these certificates will be of interest.

National Contact Points

Dr. Cristoph BRENN (Federal Ministry of Justice)
Fax: 52152 2727

Mag. LECHNER (Federal Chancellery)
E-mail: georg.lechner@bka.gv.at"

Belgium

Digital Signatures in Belgium

As a part of the "AGORA" project under the Prime Minister's office, the Belgian Government is developing an infrastructure for the use of digital signatures in Federal Government administration. This

project was initiated in 1997, and it continues in 1998.[7] All the technologies which are currently used and which permit the electronic signing of a document are available in Belgium. Digital signatures will be legally accepted and considered as equivalent to the manuscript signature in the near future, following the approval on 12 June 1998 by the Belgian Federal Council of Ministers of a draft law concerning the activities of "qualified certification authorities" for the use of digital signatures.[8] The draft Law, which will provide the framework for the use of digital signatures in Belgium, is currently before the Parliament. The main principle behind this legislation is that any natural or legal person may apply to a certifying agency (computer firm, bank insurance company, security firm, etc.) for a digital signature certificate which will identify that person and thus assign responsibility for messages sent. The service or department issuing digital signature certificates is not regulated and does not need to be licensed. Certifying authorities that wish to be officially recognised, i.e. on a voluntary basis, may be approved by a public agency. The criteria for such approval will be set forth in an Implementing Order for the draft Law once the latter has been passed by the Belgium Parliament.

The draft law sets out the minimum content for a certificate in Belgium. This will be: subject (holder of a certificate) name; public key of the subject; reference to the algorithms which are necessary for using the public key of the subject; unique identity code of the certificate; operational period of the certificate (beginning and end); identification of the certification authority (CA) and of its qualification; other information with the indication whether or not it is confirmed by the CA. Liability rules in Belgium state that the holder of a certificate is liable for the integrity, confidentiality and usage of his private key: in case of doubts about the confidentiality or the integrity of the information validity, the holder shall immediately request a suspension or revocation of the certificate. After revocation (or suspension) of a certificate or after its expiration date it is not authorised to use the corresponding pair of keys. The qualified CA is liable for the integrity, security, interoperability (technical means and expertise) and availability of financial warranty and insurance within certain limits to be fixed by the public authorities. The qualified CA should also be independent of the service users. With regard to cross-border recognition of certification, the Belgian law sets out that a certificate issued by a CA located in another European State (within the single market) is considered as equivalent to a certificate issued by a CA qualified in Belgium whether it presents the same level of security or not. Outside the single European market, mutual recognition agreements will be negotiated.

General

A Royal Decree authorises the *Banque Carrefour de la Sécurité Sociale* (the Federal Office which transits and gives information to Social Security Administrations) to approve Certification Authorities; these approvals are provisional and only concern social security. Concerning all approved Certification Authorities, a draft law concerning the activities of approved certification authorities for the use of digital signatures should be submitted to the Parliament in the near future (see clause 6). At this moment there are no published criteria, the observance of which render electronic documents or signatures admissible for evidentiary purposes. Common law applies. In commercial relationships for example, this signifies that all means of evidence are admissible. Between merchants there is therefore no problem to commit juridical acts in an electronic way; it is up to the Courts to admit these facts as evidence. In the private sector, there are several organisations that issue digital certificates for public use: Belgacom, Belsign, Publilink and Isabel. These four Certification Authorities have been provisionally approved by the *Banque Carrefour de la Sécurité Sociale*.

7. See http://www.agoraproject.org.

8. See http://belgium.fgov.be and http://www.law.kuleuven.ac.be/icri/.

Belgium does not in general use authentication technologies or mechanisms in the electronic delivery of government services to citizens. However, there are some specific applications: for example: the "Dimona-project" of the *Office National de la Sécurité Sociale* enforces the use of digital signatures and digital certificates to secure the "immediate recruitment declarations" that employers must send to the *Office National de la Sécurité Sociale*. There is also a social security card. It is a smart card holding personal information on citizens, such as identity, social security number, etc. This card, however, does not currently use any digital signature or public key based authentication procedures.

In the area of authentication and certification the Belgian government has proposed two drafts:

- A draft law concerning the activities of approved Certification Authorities for the use of digital signatures: this proposal aims to establish a legal framework for the use of electronic signatures. It was approved by the Council of Ministers on 26 March 1999 and will now be discussed by Parliament.
- A proposal to amend the Civil Code provisions about evidence: the most important provision of the proposed law is that, in the future, a signature will no longer be considered as a concept restricted to a handwritten signature but that it can be "every transformation of data from which follows with certainty the identity of the author and the integrity of the content". An electronic signature will be considered as a legal valid signature, equivalent to the handwritten signature.

Developing an infrastructure for the federal administrations: the Agora project

This project initiated by the Prime Minister's Office and the Belgian Government concerns the infrastructure to be developed for the use of information society technologies, in particular digital signatures in Federal Government Administrations. The purpose is to create the possible interoperability between the Certification Authorities in compliance with the European and Belgian Law. The first phase of this project was completed with an agreement (August 1998). The second phase must be completed by the end of 1999. In the absence of relevant legislation, Belgacom, Isabel, Belsign and Publilink have developed their own model for electronic authentication. These models are generally supported by industrial common standards.

Private contractual agreements

As a result of the lack of specific legislation, there are many uncertainties concerning the extent to which one can use electronic documents, electronic signatures, etc. As there is no specific law regarding standards or procedures, parties are free to set their own. However, these may not derogate from common (general) laws and international generally recognised standards. Parties who enter into an agreement that sets standards, procedures or uses that differ from those set forth in national laws and regulations may attempt to gain redress under the national legal system, unless, in the particular circumstances, the national law is compulsory (i.e. one may not derogate from it in a contractual agreement). Special evidentiary standards do not apply to evidence of validity and authenticity offered to a judicial or administrative proceeding in Belgium.

Standards

No Belgian certification authority (private organisation) has developed standards for electronic authentication. For granting the accreditation the *Banque Carrefour de la Sécurité Sociale* has developed certain criteria. Until now, these criteria have not been public (see clause 2). There are no laws, regulation or private sector mechanisms in Belgium which govern the development or setting of standards for digital signatures, electronic signatures, or other kinds of electronic authentication. At their own initiative, some Belgian Certification Authorities (for example: Belgacom) participate in national and international standard organisations (for example: European Electronic Signature Standardisation Initiative). Belgacom, Publilink, Isabel and Belsign also participate in the Agora-Project. Voluntary accreditation schemes have been created in Belgium by law (BELCERT for the accreditation of bodies operating certification of quality systems, products, or personnel; BELTEST for the accreditation of test laboratories and inspection bodies; BKO/OBE for the accreditation of calibration laboratories).

Certification Authorities

As yet, no measures are being taken to evaluate and approve or accredit certification authorities in Belgium. In the social sector, the *Banque Carrefour de la Sécurité Sociale* has developed its own set of procedures and rules to accredit Certification Authorities in order to deliver digital certificates to secure electronic communications towards the Social Security Institutions. The common rules of liability currently apply to the activities of certification authorities in Belgium. Concerning the responsibility of Certification Authorities, the draft law foresees that a minimum and maximum amount will be determined in a royal decree. The approved CA will be liable for the following:

- Integrity, security, interoperability (technical means and expertise) and availability of financial warranty and insurance within certain limits to be fixed by the public authorities.
- Independence towards the service users.

Global Authentication

With regard to global authentication, the draft law determines that a certificate delivered by a European certification authority will only be considered as equal to a certificate delivered by a Belgian approved Certification Authority.

National Contact Points

- Ministère des Affaires économiques
  Administration de la Qualité et Sécurité

M. Ph. DEGAVRE, Ingénieur
Bd E. Jacqmain 154
1000 Bruxelles
Tel.: 32 2 206 47 09
E-mail: ph.degavre@pophost.eunet.be

M. P. STRUMELLE, Conseiller adjoint
Rue de l'Industrie, 6
1000 Bruxelles
Tel.: 32 2 506 63 01
E-mail: pierre.strumelle@pophost.eunet.be

Canada

Authentication

The Personal Identification Number (PIN), combined with a token such as a bank card or debit card, is perhaps the method most widely used by consumers to establish identity in an electronic transaction. In Canada, this is currently the standard method for authenticating a cash withdrawal from an automatic cash dispenser, a debit card transaction (e.g. Interac network), or a banking or payment transaction carried out via an automated banking machine (ABM). When a touch-tone telephone is used to make such transactions, only an account number and a PIN can be used. However, it is the Government of Canada's view that a higher degree of authentication is required for many classes of transactions. In particular, digital signature technologies are required to "sign" an electronic document and provide a better means to establish the authenticity of the originator.

Certification

The Government of Canada believes that the acceptability of electronic signatures is likely to depend on the reliability and integrity of the systems that create them. The ITU X.509 standard (ISO 9594-8) has been adopted by the Standards Council of Canada as a National Standard. The federal government is of the opinion that, currently, only X.509 v.3 based digital signature technology meets the test of a secure electronic signature, for purposes of use within the government and with its clients. This is also the view of a number of provincial governments and some private sector organisations in Canada such as Scotiabank. Canada knows of no other standard that has gained such widespread acceptance. It is the Government of Canada's view that what makes a secure electronic signature trustworthy is the use of the technology in conjunction with a reliable Certification Authority (CA). Canada envisages a network of CAs operating in public and private sector organisations, which will offer a range of authentication and certification services to organisations that cannot afford to set up their own CA, or choose to contract out this function. Accreditation and cross-certification of CAs will become key issues in this environment. The federal government will encourage market-based solutions wherever possible.

A certificate policy (CP) states what assurance can be placed in a certificate; a certification practice statement (CPS) states how a CA establishes that assurance. Certificate policies constitute a basis for the accreditation of CAs; each CA is accredited to support one or a set of certificate policies, which it proposes to implement. Certificate policies are also used to establish cross-certification, i.e. a trust relationship between CAs. When CAs issue cross-certificates, one CA will assess and recognise a set of

certificate policies of the other CA. Chaining of CAs in the cross-certification process raises important policy and liability issues; these need to be discussed and resolved before chaining can be accepted. The Government of Canada believes that in order that electronic commerce may be conducted securely and efficiently across jurisdictions, PKIs must be interoperable with one another, and cross-certification of CAs operating in different jurisdictions must be facilitated. There is a need for the harmonisation of approaches and policies between the Canadian federal and provincial governments, for purposes of interoperability and compatibility of electronic authentication systems. For this reason, a joint Federal-Provincial-Territorial PKI Working Group, under the Public Sector CIO Council, has been set up to develop common principles and a framework for the co-ordination of policy, standards and technology, for interoperability and cross-certification among the PKIs being developed. A Canada-US PKI Liaison Group has been set up to promote information exchange, collaboration and future joint pilots between departments and agencies of the Canadian and US federal governments.

Authentication, Certification and Related Services

The areas of potential application for authentication and certification services in Canada are very broad. They include many forms of government-to-clients (businesses and citizens), business-to-business and business-to-consumer transactions. Major government applications include statutory filings and applications (e.g. income tax, motor vehicle and drivers' licenses, business incorporation, goods and services tax), collection of fees and benefit payments (e.g. employment insurance, old age pensions), and procurement of goods and services (e.g. electronic tendering systems like MERX). Such services could also be extended to Electronic Funds Transfer (EFT) systems, consumer Electronic Payment Systems, and to the traditional forms of Electronic Data Interchange (EDI) between businesses linked via a supply chain. Currently, the latter forms of electronic transactions are almost entirely carried out over private, closed user group or value-added networks, often using proprietary authentication methodologies. As many of these applications and services migrate to open networks, the need for independent authentication and certification services will grow.

It is the Government of Canada's view that the requirements for ensuring the integrity of data for electronic transactions become particularly important for commerce carried out over open networks, such as the Internet. Unlike transactions carried out over private or closed user group networks (e.g. S.W.I.F.T. or the VISA, MasterCard and Interac networks), those carried out over open networks like the Internet cannot currently be guaranteed a specific quality of service (e.g. delivery assurance, time of delivery, etc.), and security becomes the responsibility of the end user. Network security solutions include the use of the Secure Socket Layer (SSL) over the Internet, and the use of secure Virtual Private Networks (VPNs). Since SSL support is embedded in the new generation of Internet browsers, it is being increasingly used for the exchange of credit card information between buyers and trusted vendors like Amazon.com. Although digital certificates are currently optional within SSL, this feature is not widely used, for operational and other reasons. An international group of companies (including Visa, MasterCard, IBM, Microsoft, Netscape, etc) has developed the Secure Electronic Transaction (SET) protocol, to ensure the security and privacy of payment card transactions over the Internet and various pilots and trials are underway. Leading edge banks like Canada's Scotiabank have already begun to use PKI technologies to offer secure on-line banking and brokerage services to their customers over the Internet.

Legal and Policy Issues under Consideration

In general, Canadian common law can be interpreted to apply to activities conducted electronically. This means that the current common law rules on liability apply to activities by certification authorities. CAs

may attempt to limit their liability by contract (e.g. through certificate policies and subscriber agreements), but limitations will be subject to common law. There is no legislation in Canada that sets out specific requirements for certification authorities or the issuance and management of public and private keys. Canada's Cryptography Policy calls for freedom of choice in the development and use of products and services, and no mandatory key backup. The Policy also states that the federal government will not introduce a mandatory licensing scheme for CAs; instead the Policy calls for an industry-led accreditation regime.

The Government of Canada believes that in order to help electronic commerce to flourish, the legal framework must be adapted to allow a trustworthy electronic signature to have a legal effect similar to a paper-based signature. Since the application of current laws to paperless transactions may lead to uncertain results, the Government of Canada is acting to make adjustments to statutes and regulations where required, to bring greater certainty to the use of information technology and electronic commerce, and to provide for the electronic alternative to paper. For this purpose, in October 1998 the Government of Canada introduced Bill C-54, the *Personal Information Protection and Electronic Documents Act*. The new legislation is expected to pass by the summer of 1999. It is designed to permit the use of electronic technologies for government service delivery and, in some limited instances, to require the use of "secure electronic signatures" in dealing with the federal government (e.g. for seals, original documents, sworn statements and notarial documents). Currently, there are over 300 federal statutes in Canada which contain provisions requiring documents, such as information returns and notices, to be "in writing", "in prescribed form", "authorised", "notarised", "certified", or "signed". Part 2 of Bill C-54 sets out the legislative scheme by which requirements in federal statutes and regulations that contemplate the use of paper, or do not expressly permit the use of electronic technology, may be administered or complied with in an electronic environment. It grants authority to the appropriate authorities to make regulations about how those requirements may be satisfied using electronic means. Rather than have each department or agency amend legislation piecemeal, Bill C-54 will enact a set of general or global provisions, authorising the use of electronic communications and electronic service delivery, which individual departments or agencies can opt into, when they are ready to do so. Two general enabling provisions are also proposed. The first would authorise a Minister to use any electronic means to create, collect, store, transfer, receive or otherwise handle documents or use information technology; the second would also permit payment of a fee by electronic means, in a manner specified by the Receiver General of Canada.

Part 2 of Bill C-54 grants the Governor in Council (i.e. the government) authority to make regulations prescribing technologies or processes for the purpose of the definition of "secure electronic signature", and also describes the functional characteristics which such a technology or process must possess. In Canada, many legal rules and the law of evidence assume the existence of paper, signed or original records. As more and more activities are carried out by electronic means, it becomes increasingly important that evidence of these activities be available, to demonstrate the legal rights that flow from them. The Uniform Law Conference of Canada (ULCC) has prepared a draft Uniform Evidence Act, which evaluates the integrity of an electronic record by considering evidence of the reliability of the record-keeping system which generated the record. Part 3 of Bill C-54 amends the *Canada Evidence Act*, consistent with the draft ULCC Uniform Evidence Act, to facilitate the admissibility of electronic documents, to establish evidentiary presumptions related to secure electronic signatures, and to provide for the recognition as evidence of notices, acts and other documents published electronically by the Queen's Printer. Bill C-54 grants authority to make regulations establishing evidentiary presumptions in relation to electronic documents signed with secure electronic signatures, concerning the association of signatures with persons, the validity of the certificate, and the integrity of the information contained in a document signed with a secure electronic signature. These presumptions should improve certainty for

persons who use and rely on secure electronic signatures. These presumptions would only apply to certificates issued by certain certification authorities and to the signatures referred to in those certificates. Reliable certification authorities would include those operating under the Government of Canada Public Key Infrastructure (GOC PKI), similar provincial/territorial PKIs, and those CAs which have been cross-certified to, or are otherwise recognised by these PKIs. Potential examples could include Canada Post and the national banks. The new legislation will not dictate any other aspects of CA operations.

These efforts are aimed at assisting and facilitating the electronic delivery of services by the federal government. Provincial governments would need to make similar changes, as well as updates to statutes where required. The provinces are planning to address these issues along similar lines, through the ULCC. With these efforts, legal issues will become less of an impediment to electronic commerce and the development of CA services in Canada, than concerns over market take-up, technology evolution and physical risks. These products and services are at an early stage of development, and the Government will encourage continued investment and innovation by the private sector, and use by citizens and businesses.

Public Sector Approaches and Private Sector Initiatives

The Canadian federal, provincial and territorial governments have endorsed the goal of making on-line delivery both a priority and the preferred mode for those government services that lend themselves to electronic delivery. The Government of Canada (GOC) is committed to using information technology to provide innovative service delivery to Canadians and to improve the efficiency of government operations. The preferred mode of doing business with the Government of Canada will be electronic. The Government of Canada Public Key Infrastructure (GOC PKI) is a government-wide implementation of an information technology security infrastructure which will provide the confidentiality, data integrity, authentication and non-repudiation features needed to conduct the electronic business of government. The GOC PKI provides for cross-certification arrangements to ensure the interoperability of CAs within the federal government, and cross-certification agreements will be established as required with external partners such as businesses, provincial and territorial governments and foreign countries. An interdepartmental PKI Implementation Team of committees, working groups and a Task Force is in place and operating to develop the GOC PKI. The Communications Security Establishment (CSE) has been designated as the Central Certification Facility ("root" Certification Authority). Several other federal government CAs are currently functioning under the GOC PKI. The policy framework for the GOC PKI, currently being finalised, includes the development of a model Certificate Policy (completed), model External Subscriber Agreements, Cross-certification Agreements (internal and external), and Minimum Terms and Conditions for the Procurement of Certification Authority Services. These model policy instruments, and the necessary legal framework for the electronic delivery of federal government services, are expected to be in place by the summer of 1999. From the growing number of specific pilots and projects in PKI being undertaken by various Federal departments and agencies, eleven have been selected as PKI Pathfinders; projects which are pioneers in breaking new ground, leaders in taking initiative and innovators in fostering change. More information on all aspects of the GOC PKI, including the model Certificate Policy, is available at the Web site www.cio-dpi.gc.ca.

The GOC PKI is based on technology developed by Entrust Technologies Ltd (ENTRUST). However, cross-certification and the commitment to open standards and commercial, off-the-shelf products provide the opportunity for alternatives to be equitably considered. The Government of Ontario PKI is also based on the Entrust technology platform. Both the Ontario and Quebec Provincial Governments are undertaking significant PKI initiatives, including a number of major pilots. The Alberta Government has now initiated several pilots, and other provincial governments are engaged in assessing their PKI possibilities. These federal and provincial projects are leading the way in the practical application and use

of PKI in government business in Canada. In the Canadian private sector, Scotiabank has pioneered the innovative use of PKI in the roll-out of its on-line banking and brokerage services, with some 70 000 users as of the summer of 1998. A customer can access bank accounts, pay bills and make stock transactions securely over the Internet. Scotiabank claims that it is currently the largest Certification Authority in the world.

International Aspects

Appropriate fora for the discussion and resolution of issues related to electronic authentication and certification could include: the OECD for discussing a wide range of policy related issues; UN agencies like UNCITRAL for exploration of the legal issues related to digital signatures and certification authorities; ISO, in conjunction with the IETF, for technical standards related discussions; and WTO, UNCTAD and APEC, which are deeply interested in issues related to the use of secure electronic commerce to support international trade. Pilot projects are required to demonstrate the use of electronic authentication and certification across international boundaries. Technical interoperability is the first necessary step towards cross-certification. A pilot project is being conducted between Industry Canada and the Singapore National Computer Board, to demonstrate the technical interoperability between the CAs of these two organisations.

National Contact Points

- Helen McDonald
  Electronic Commerce Task Force
  Industry Canada
  Government of Canada
  Tel: 01-613-990-4732
  E-mail: mcdonald.helen@ic.gc.ca.

- Joan Remsu
  Senior Counsel Public Law Policy Section
  Justice Canada
  Tel: 01-613-946-3118
  E-mail: joan.remsu@justice.x400.gc.ca (for inquiries on legislative initiatives).

- Michael de Rosenroll
  PKI Interdepartmental Task Force
  Tel: 01-613-957-2535
  E-mail: derosenroll.michael@tbs-sct.gc.ca (for inquiries on GOC PKI)

Czech Republic

The Czech Republic is due to join the European Union after 2000. For this reason, it has carefully followed the European Union approach to harmonise its laws, and other aspects of authentication and certification, with the EU rules. The Czech Republic does not as yet have a specialised agency to deal with these issues. The Office for the State Information System has been requested by the Czech Government to prepare a certification law in close co-operation with both the public sector (in particular

with the Ministry of Trade and Industry, the Ministry of Finance, and the Ministry of Interior) and the private sector, as soon as possible. The Czech Republic follows the laws of the EU and UNCITRAL in the field.

General

Following upon the October 1998 *Ministerial Declaration on Authentication for Electronic Commerce*, the 1996 UNCITRAL Model Law on Electronic Commerce was sent out to ministries and governmental agencies with a request for comments. In this respect, the Czech Republic is starting to take steps to amend, where appropriate, technology or media specific requirements in current laws or policies that may impede the use of information and communication technologies and electronic authentication mechanisms, giving favourable consideration to the relevant provisions of the 1996 UNCITRAL Model Law on Electronic Commerce. As yet there is no specific law or regulation concerning digital signatures, electronic signatures, or other kinds of electronic authentication or any published criteria, the observance of which render electronic documents or signatures admissible for evidentiary purposes. There are several firms (primarily Internet providers) offering digital certificates for public use in the Czech Republic. The most important of them is certification authority 1.CA (www.ica.cz; PVT, a.s., Kovanecka 2124/30, Prague). As yet the Czech government does not use authentication technologies or mechanisms in the electronic delivery of government services to citizens. Initiatives exist in the area of authentication and certification, for example the Office for the State Information System in close co-operation with the private sector [Association for Information Society] has been preparing the law on electronic signatures. With regard to private sector models for electronic authentication CA has its own (complex) rules regulating the use of electronic certificates.

Private contractual agreements

Parties are free to agree standards, procedures and uses and there is no legislative support from national law. There are no evidentiary standards that apply to evidence of validity and authenticity offered to a judicial or administrative proceeding.

Technology requirements

National law or regulation has not yet identified certain electronic authentication technology as “secure”. However, the National Security Agency has been preparing “The Notice of NSA about cryptographic protection and the certification of cryptographic tools”. The Notice is put into force from May 1999. The Law 148/98 – “Information Protection Act” differentiates between levels of security, it provides the framework law for classification and protection of information in the Czech Republic. The Law and other corresponding laws, notices and amendments define information which is classified as top secret, confidential and restricted should be protected.

Standards

As yet there are no widely accepted standards or rules for electronic authentication. However, some standards have been used in specific projects and cases. There are not as yet laws, regulations or private sector mechanisms governing or developing/setting standards for digital signatures, electronic signatures, or other kinds of electronic authentication. Compliance with any standards is not mandatory. The private

sector plays a role in developing and certifying standards for digital signatures, electronic signatures, or other kinds of electronic authentication. This is done through consultation and reviews of proposals as well as participation in work groups.

Certification authorities

The new law on electronic signatures will address some of the issues concerning certification authorities. As yet there are no laws or regulations that govern or set requirements for licensing or accrediting "certification authorities".

National Contact Points

- Jitka Urbanová
  Department of International Co-operation
  Office of the State Information System
  Havelkova 22, 130 00 Praha 3
  Czech Republic
  Tel: +420 2/ 21008 203
  Fax: +420 2/ 2422 0613
  E-mail: urbanovaj@usiscr.cz.

  Alternatively, enquiries can be addressed to The Bureau for State Information System.

Denmark

The Danish Ministry of Research and Information Technology presented a Draft Bill for an Act on Digital Signature in February 1998. The Draft Bill is based on the assumption that growth in electronic commerce requires a legal framework which will allow for the creation of binding agreements on open networks, such as the Internet. The purpose of the Draft Bill is to establish a secure environment for the use of electronic communications to form binding legal transactions. In particular, it aims to allow such communications to take place in an environment where the identity of the sender and the addressee and the integrity of the message content are ensured. The goal is to provide users of digital signatures secure solutions that are easy to use. The Draft Bill also obliges public authorities to offer digital communications for public services. The Draft Bill creates an environment for the use of public key-encryption technology. It contains provisions on key certificates (relating to barring, time of expiration and area of application), the legal effects of digital signatures, certification authorities (relating to authorisation, responsibilities and liabilities), time stamping, supervision, complaints and sanctions. The Draft Bill was circulated among many organisations and Ministries in Denmark. As a result of the hearing the draft was revoked. The Ministry of Research and Information Technology is currently working on a new draft based on the provisions of the draft EU Directive on Electronic Signatures.

With respect to the legal effects of digital signatures, the consultation process indicated that a thorough investigation of the consequences of digital signatures is necessary, for example in the context of public law, contract law and consumer protection law. The Ministry of Justice, which is responsible for such laws, has established a committee of experts to consider the possibility of legislation on the legal effects of digital signatures. The provisions on the legal effects of digital signatures that were included in the Draft Bill will not be part of the Bill that will be introduced to Parliament by the Ministry of Research and

Information Technology. The Ministry of Research and Information Technology has invested DKK15 million in 9 pilot projects on the use of digital signatures. Three thousand users will be involved, including private citizens, students, farmers, and small and large enterprises. The Ministry has established the standards to be used for the digital signatures. The aim is to provide the basis for a coherent infrastructure for digital signatures and to support the diffusion of smart cards in Denmark. The pilot projects have started at the beginning of 1999 and will terminate as pilot projects during the summer 2000.

National Contact Point

- Mr. Kenneth Smith Petersen / or Mr. Claus Jakobsen
  Head of Section, Forskningsministeriet (Ministry of Research and Information Technology)
  Bredgade 43
  1260 Copenhagen
  Denmark
  Tel: +45 33 95 52 34
  Fax: +45 33 93 84 03
  E-mail: ksp@fsk.dk / cja@fsk.dk

Finland

Authentication and Certification

There is no law in Finland dealing specifically with electronic authentication. All existing methods to establish identity in the electronic environment have been created to serve the needs of the private sector, and they are usually for closed user groups. A number of electronic signature products are also commercially available in Finland. The "Electronic Citizen Card" is a project of the Finnish Government aimed at all Finnish citizens and is intended to entail a relatively modest user cost. Apart from the Electronic Citizen Card, certification services in Finland are designed by, and for the needs of, the market. The Finnish court system accepts all kinds of evidence, so the value of a digital signature in proving a transaction is determined by the judge on a case-by-case basis. Finland believes that the market for electronic signatures and certification services is going to be huge in all sectors of society, including the public sector. There are requirements currently in place for ensuring the integrity of data for electronic transactions and commerce because of the evidence rules in the Finnish court system. However, as new sophisticated certification services emerge, their use will probably be quite widespread.

Legal and Policy Issues under Consideration

The principles of freedom of contract and free evaluation of evidence allow for quite extensive use of digital signatures in transactions under private law in Finland. There are, however, certain transactions, such as most transactions relating to immovable property, where the use of a particular form is required by statute. Although form requirements often preclude the use of a digital signature, it is not expected that many of the transactions where a particular form is required will be entered into over an open data network in the near future. The need for regulation of digital signatures and certification organisations was recently surveyed by a Working Group appointed by the Finnish Ministry of Justice. In their report, published in March 1998, the Working Group underlined the importance of the principle of non-regulation: legislation should not establish unnecessary barriers to modern transaction methods. The

necessity of retaining formal requirements currently restricting the use of digital signatures should be considered on a case-by-case basis. There are no special laws or regulations addressing the issues of risk and liability allocation for losses in connection with the use of electronic signatures in Finland. Currently these issues are dealt with by applying the general principles of private law and the pertinent statutes, in particular the Contracts Act, and, in the absence of any contractual arrangement between the parties concerned, the Damages Act. Currently there is some uncertainty as to the precise legal effects of digital signatures and, in particular, the exact scope of the rights and responsibilities of the parties involved in electronic commerce. This uncertainty is largely due to the absence of special laws or regulations and the dearth of case law on the interpretation of the general statutes in force. At the moment, however, no legislative amendments are underway. The necessity and scope of any amendments will eventually be evaluated taking into consideration, *inter alia*, the legal instruments adopted at both the European Community and global levels.

Public Sector Approaches and Private Sector Initiatives

Finland is actively involved in the drafting of the forthcoming European Parliament and Council Directive on a common framework for electronic signatures. There is no intention to propose national legislation on certification activities before the implementation of this Directive, except for the amendments necessary for the proper functioning of the Electronic Citizen Card system. These relate mainly to the organisation and tasks of the Population Register Centre.

General

Following the October 1998 *Ministerial Declaration on Authentication for Electronic Commerce*, Finland has taken steps to amend, where appropriate, technology or media specific requirements in current laws or policies that may impede the use of information and communication technologies and electronic authentication mechanisms. Favourable consideration was given to the relevant provisions of the 1996 UNCITRAL Model Law on Electronic Commerce. Legislation which states supplying trusted third party services as a governmental task, run by the Population Registry Centre, was accepted in February 1999. The system uses an electronic identity card as an identification device. An identification card is not compulsory. It can be used in applications of electronic commerce and electronic transactions with public authorities. The Bills of electronic identity card and electronic transactions with public authorities will be given before July 1999. Finland has no specific law or regulation concerning digital signatures, electronic signatures, or other kinds of electronic authentication. However, the Finnish legal system allows the use of digital or electronic signatures in private business without restriction. Electronic identification, however, without PKI infrastructure, is used widely in the banking business. Public agencies need special law for using electronic signatures in government.

Although as yet there is no public or private sector body that issues digital certificates for public use, at the beginning of December 1999 the Population Registry Centre will begin to issue electronic identity cards. There are also several private certification authorities, but no-one has begun the service yet. There is, for example, technological readiness to use digital signatures by mobile phones. There was a decision taken by the government on 5 February 1998, which states the government's intention to provide a significant amount of government services to citizens using authentication technologies or mechanisms in the electronic delivery of those services by the year 2001. The Ministry of Finance and the Ministry of Interior are responsible for issuing these services. The Ministry of Justice has the responsibility of developing appropriate legislation. Private sector models for electronic authentication are in operation or

under development in Finland. Most banks have identification systems of their own. A significant amount of transactions in banks are made through the Internet. Banks use changing passwords and as yet current banking systems do not use certificates. There are, however, two joint projects with the Population Registry Centre and a bank to use an electronic identity card as an identification tool.

Technology requirements

Finland's laws and regulation do not specifically approve a particular kind of electronic authentication technology or mechanism. Parties who use electronic authentication methods that are not specifically approved by law or regulation may establish the validity and authenticity of that method by offering evidence of its reliability in a judicial or administrative proceeding. In general, there are no legally stated prerequisites for evidence. The court has freedom to accept or reject any evidence. The evidential value is considered on a case-by-case basis. If parties in judicial or administrative proceedings use an alternative to legislatively or administratively approved methods of electronic authentication, the courts and public authorities will consider on a case-by-case basis which method of authentication is accepted. There is, however an intention to set some legal criteria to electronic authentication and electronic signatures. These criteria will be objective, e.g. demands the use of the PKI methods and sufficiently long keys. A bill about the matter will be presented in June 1999.

Standards

National standards for electronic authentication not yet been developed by the public or private sectors in the country. However, there will soon be a public certification authority, the Population Registry Centre. The Centre will use common Nordic specifications, called SEIS. These specifications do not, however, have the status of a national standard. They are expected to form a *de facto* standard. The law about the Population Registry Centre defines the content of a certificate. This does not, however, limit the use of other type of certificates. It is expected that these specifications will form a *de facto* standard. Compliance with any standards is not mandatory in Finland. Therefore failure to follow a national standard will not give rise to liability in civil proceedings, or increase the likelihood that a party will be held liable for the use of an alternative standard. The private sector plays a role in developing and certifying standards for digital signatures, electronic signatures, or other kinds of electronic authentication. There are private companies who use different kind of specifications. National laws and regulations permit private-sector bodies to certify compliance with legislatively- or administratively-approved standards. This is possible because there is no regulation of such procedure of certification. Merita-Nordbanken is an example of a private sector initiative which concerns standards and related issues in the area of authentication. It offers its certification services, that are based upon changing passwords, to companies and public authorities.

Certification authorities

As yet there are no measures being taken to evaluate and approve, or accredit, certification authorities (or other providers of trusted services) in Finland.

Global authentication

National laws or regulations recognise digital signatures, electronic signatures, or other kinds of electronic authentication used in other countries. These can be used in private business. There are no procedures in

place in Finland to recognise foreign providers of similar services such as providers of trusted services related to digital signatures, electronic signatures, or other kinds of electronic authentication. There are not as yet any central public or private sector bodies that can cross-certify certification authorities at the national or sub-national level. However, national laws or regulations do not place limitations on cross-border recognition of electronic authentication in private business transactions. Neither are limitations placed on cross-certification between certification authorities operating in Finland and certification authorities in other countries.

National Contact Points

- Electronic signatures in general:
  Mr. Joel Jaakkola
  Ministry of Transport and Communications
  Tel: +358 9 1609151
  Fax: +358 9 1602588
  E-mail: joel.jaakkola@lm.vn.fi.

- Electronic Citizen Card:
  Mr. Kaarlo Korvola
  Ministry of Finance
  Tel: +358 9 1603209
  Fax: +358 9 1603229
  E-mail: kaarlo.korvola@vm.vn.fi.

- Technical aspects:
  Mr. Harri Rasilainen
  Telecommunications Administration Centre
  Tel: +358 9 6966824
  Fax: +358 9 6966410
  E-mail: harri.rasilainen@thk.fi.

France

In France, the standard method for authenticating a cash withdrawal from an automatic cash dispenser, a debit card transaction, or a banking or payment transaction is the personal identification number (PIN). However, when an electronic document must be "signed", the use of digital signature technologies is necessary in order to make sure that the document is authentic and has not been altered or falsified, and that the author of the document and the person who signs it are one and the same person. The French legal framework will have to be adapted to take into account new technologies and the development of electronic commerce so that electronic signatures can have, to some extent, a legal effect similar to that of a paper-based signature. Currently, there is no definition in French law of a "signature". A recent report on "Internet and digital networks" issued by the *Conseil d'Etat* at the Prime Minister's request[9], suggests that the notion of "signature" should be defined in French law according to the various functions a

[9] Internet and Electronic Networks, study adopted by the General Assembly of the *Conseil d'Etat*, 2 July 1998, available on the Internet since 8 September 1998, see http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm.

trustworthy signature is meant to play: i.e. to establish the identity of the originator, and his or her consent to the content of the document. The French Government believes that only reliable electronic signatures can foster user confidence to facilitate the development of global electronic commerce. The acceptability of electronic signatures depends to a great extent on the use of sophisticated technological security devices operated in conjunction with trustworthy Certification Authorities (CA). Accreditation and cross-certification of CAs will become key issues for the private and public sectors.

The French Telecommunications Law n° 90-1170 dated 29 December 1990, amended by law N° 96-659, dated 26 July 1996 (article 17) contains provisions covering the use of cryptography for authentication, particularly the supply of digital signature products and services subject to information procedures, and the import and export of digital signature products and services[10]. The new legislation has completely freed the use of cryptography, provided it is used exclusively for digital signatures, to establish the authenticity of a message, its irrevocability and to control its integrity. Under this regulation, the provision of cryptographic technologies that only ensure a digital signature function is subject to a simplified registration system. The provider can immediately market the product when it is specified in the registration that the system cannot be used for confidentiality functions.

Legal and Policy Issues under Consideration

Since the application of current laws to paperless transactions may lead to difficulties, the French Government is aware of the need to make adjustments to statutes and regulations where required, to provide for the electronic alternative to paper. Indeed, in France, many legal rules and the law of evidence assume the existence of paper, signed or "original" records. Currently, there are a number of statutes in France which contain provisions requiring documents -- such as sworn statements, notarial documents, information returns and notices -- to be "in writing", "in prescribed form", "authorised", "notarised", "certified", or "signed". The rapid development of activities carried out by electronic means makes it necessary for the information that flows from electronic activities to be able to be taken into consideration as evidence. The French Department of Justice is preparing a bill to amend the French law of evidence contained in the Civil Code. It proposes three statutory presumptions concerning: the authentication of the user of the digital signature, the integrity of the document signed by digital signature technology, and the functional equivalence between a written document and an electronic one.

International Issues

France is committed to the drafting of the forthcoming European Parliament and Council Directive on a common framework for electronic signatures. The implementation of the Directive may lead to some amendments of the French legislation.

Studies and Reports

In December 1997, Mr. Francis Lorentz was appointed by the Minister of Economy, Finance and Industry to examine the key issues of electronic commerce and to identify the barriers to its development. He issued a report on "Electronic commerce" in which he proposed amendments to the legal framework in order to foster the growth of global electronic commerce. In its May 1997 report on "Legal issues linked with Electronic Payment Systems", the National Council for Credit suggested that the Civil Code must be

[10] Statutes dated 24 February. 1998, 23 March 1998.

adapted with regard to provisions requiring paper documents. A working group on electronic commerce, chaired by law professors, was asked by the Ministry of Justice to propose amendments to the current French civil legislation. Among various proposals, they suggested that an electronic message could be considered as equivalent to a paper document and that electronic evidence could be equivalent to paper evidence. In December 1997, the Prime Minister asked the *Conseil d'Etat* to look at the key legal issues related to Internet and applicable law. In its report "Internet and electronic networks", made public in September 1998, the *Conseil d'Etat* makes various proposals about how to adapt the French legal framework to facilitate the growth of global electronic commerce.[11]

National Contact Points

- Philippe Dejean
  Service Central de la Securité des Systemes d'Information (SCSSI)
  Chef de la division chiffre
  18, rue du docteur Zamenhof
  92131 Issy-Les-Moulineaux
  Tel: +33 1 41 46 37 21
  Fax: +33 1 41 46 37 01
  E-mail: 100435.673@compuserve.com

- Florence Schmidt-Pariset
  Ministère de la justice
  13, Place Vendôme
  75042 Paris Cedex 01
  Tel: +33 1 44 86 14 82
  Fax: +33 1 44 86 14 21
  E-mail: mp228-1@dial.oleane.com

- Lionel Vodzislawsky
  Ministère de l'Economie et des finances
  3-5 rue barbet de Jouy
  75353 Paris 07 SP
  Tél: +33 1 43 19 34 02
  Fax: +33 1 43 19 28 51
  E-mail: lionel.vodzislawsky@industrie.gouv.fr

Germany

The German approach to electronic commerce generally can be seen in the Electronic Commerce Initiative of the Federal Government, produced by the Ministry of Economics[12]. The German Digital Signature Act (Article 3 of the IuKDG or Multimedia Law)[13] entered into force on 1 August 1997. The

11 http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm

12. See http://www.bmwi.de.

13. See http://www.iid.de/rahmen/iukdgbt.html.

implementation of the EU Directive on Privacy is in process and will go to Parliament in summer 1999. Germany has specific laws concerning digital signatures, electronic signatures, or other kinds of electronic authentication in the form of the digital signature law and the digital signature ordinance. Many private organisations issue digital certificates for public use, but until now only Deutsche Telekom is in full conformance to the digital signature law and the digital signature ordinance. Several pilot projects involving the use of authentication technologies or mechanisms in the electronic delivery of government services to citizens are in operation e.g. electronic tax declaration, electronic health card, digital company-ID-card. There are several pilot projects on the way to implement authentication and other electronic messaging applications within the different levels of regional, state and federal administrations. See: http://www.iid.de/media@Komm.

Private Contractual Agreements

The "German Digital Signature Act" does not imply any additional legal effects concerning the use or recognition of any kind of digital signatures regardless of whether they agree with or differ from the standards set forth in the "Digital Signature Act". German Private Law upholds the principle of freedom from formal requirements. Parties are generally allowed to sign contracts also in electronic form. Even they can agree to use electronic or digital signature for the offer or approval of a contract. Only in the case of specific legal form requirements shall parties use the specific formal act, even when they would agree to a certain authentication technique. Digitally signed (or even unsigned) contractual agreements are valid as long as the specific legal regulations do not require a handwritten signature and as long as they are undisputed. If in the near future legal consequences of digital signatures are established as comparable or equivalent to the legal consequences of handwritten signatures, this will be limited to digital signatures according to the "Digital Signature Act". If parties enter into an agreement that sets standards, procedures, or uses that differ from those set forth in national laws and regulations, the parties use the national legal system to attempt to attain redress under the terms of the contract. The German "Digital Signature Act" only provides a framework in public law terms, in which digital signatures are supposed to be secure (§ 1.1 Signaturgesetz). Parties are free to make use of different technical procedures, as far as digital signatures are not required by this law as standard for offering legal recognition. Evidentiary standards apply to evidence of validity and authenticity offered to judicial or administrative proceedings. The German "Digital Signature Act" defines standards under which digital signatures can be regarded as secure. Digital signatures according to the "Digital Signature Act" can therefore rely on a security assumption that implies their validity in judicial or administrative proceedings. Parties using digital signatures that rely on standards which differ from those set forth in the "Digital Signature Act" have to prove the security of the procedures used to imply the validity of the digital signature in judicial proceedings.

Technology Requirements

The German "Digital Signature Law" is based on a public key infrastructure using asymmetric public key crypto-systems. There is no specific technology mentioned or favoured in the "Digital Signature Act". Any technology wanting to gain recognition according to the "Digital Signature Act" must meet the security requirements set forth by the Act and must be approved by an accredited authority. Anybody who wishes to use methods or technologies that do not meet these requirements can do so, but the security assumption does not apply for these methods or technologies. German law identifies certain electronic authentication technology as "secure". No requirements of local partnership or establishment exist. The German "Digital Signature Act" does not, however, mention any specific technology and therefore does not identify any technology exclusively as "secure". All digital signatures that meet the safety standards

according to the "Digital Signature Act" can rely on the security assumption and therefore have the same legal consequences. The German "Digital Signature Act" and the corresponding ordinance define mandatory requirements for technical components, mechanisms and procedural actions linked to the administration of signature keys. These functional requirements are published in the federal gazette. All technical components or systems complying with the "Digital Signature Act" need to be certified by accredited authorities. These accredited authorities also certify the compliance of security concepts of certification authorities with the "Digital Signature Act". All certified components, systems and certification authorities are published in the federal gazette. Digital signatures that rely on standards that differ from those set forth in the "Digital Signature Act" can not rely on the security assumption. Therefore evidence of the security of the procedures used needs to be presented in judicial proceedings which implies the validity of the specific digital signature.

Standards

Currently, national standards ensuring the interoperability of digital signatures are being developed, for example "Signature interoperability specification [SigI]", that incorporate different international standards as a framework. Specifications regarding digital signatures are being developed jointly by public and private bodies, although there are no laws or regulations that set technical standards other than security standards for applications that comply with the "Digital Signature Act". Failure to follow national standards will not directly give rise to liability in civil proceedings, or increase the likelihood that a party will be held liable for the use of an alternative standard. Only in cases in which parties agreed to make use of a similar standard to the "Digital Signature Act", can a party be held liable. Bodies of the private sector (accredited certification authorities) develop specifications for digital signatures that fulfil the requirements of the "Digital Signature Act". Other private bodies are developing specifications that do not, or do not completely meet these requirements (e.g. MailTrusT). Most of these standards use techniques, methods or mechanisms that have been standardised by ISO and DIN respectively and will undergo further standardisation by the said standardisation bodies. There are four authorities concerned with standards and related issues in the area of authentication. They are accredited according to the "Digital Signature Act" and three of them belong to the private sector. All accredited authorities are able to certify technical components or systems as well as security concepts of certification authorities. There is an initiative in DIN (the German national standardisation body) to specify interoperability guidelines and other technical papers.

Certification Authorities

Certification authorities that wish to offer trusted services according to the "Digital Signature Act" need to be certified by an accredited authority. Certification authorities that do not want to meet the standards of the Act do not need any kind of accreditation. Only providers of trusted services that wish to operate according to the "Digital Signature Act" need to be certified. Any entity that meets the security standards of the act can be certified by any one of the four currently accredited authorities, three of which belong to the private sector. At this time there are no specific liability rules for certification authorities in Germany. There is no need for specific liability rules, but in the case where the Directive is set into force, Germany will possibly have to add some extra rules, i.e. with regard to the provisions in art. 6.3 and 6.4 of the Directive, as far as the limitation of the transactions is concerned.

Global Authentication

Foreign digital signatures of certification schemes that meet security standards equivalent to those set forth by the German "Digital Signature Act" can be recognised through bilateral agreements. Digital signatures capable of being verified by a public signature key certified in a Member State of the European Community, or in a State party to the agreement on the European Economic Area, shall be deemed equivalent to digital signatures under the "German Digital Signature Act" insofar as they show the same level of security after implementation of the EU Directive on Electronic Signatures. For recognition of foreign providers of similar services related to digital signatures, electronic signatures, or other kinds of electronic authentication, equivalent security is necessary, including equivalent accreditation schemes and equivalent testing methods. The certification scheme, run under the "Digital Signature Act" allows only the root certification authority, the "Regulatory Authority for Telecommunication and Post" to issue cross-border certificates. There are no limitations on cross-border certification for certification schemes that do not comply with the "Digital Signature Act". As yet, there are no private sector models for cross-certification of certification authorities. Private sector models for cross-certification of certification authorities do exist, for example DFN - Cert, banking systems (HBCI) to name just a few. There are no regulations or limitations on cross-border certification nor any kind of cross-certification for certification schemes that do not comply with the "Digital Signature Act". Only cross-certification within the certification scheme according to the "Digital Signature Act" is limited.

National Contact Points

- Federal Ministry of Economics and Technology
  Mr. Hubertus SOQUAT
  D-10115 Berlin, Scharnhorststrasse 36
  Tel: +49 30 2014 - 9 (direct -71 39)
  Fax: +49 / 30 / 2014 - 55 93
  E-mail: soquat@berlin1.bmwi.bund400.de

- Federal Ministry of the Interior
  Mr. Wendelin BIESER/ Mr. Andre REISEN
  Phone: +49 228 681-0 (direct -44 57 and -5109)
  Fax: +49 /228 / 681- 42 57
  E-mail: wendelin.bieser@bmi.bund400.de
  andre.reisen@bmi.bund400.de

- Regulatory Authority:
  Regulierungsbehoerde fuer Telekommunikation und Post
  Mr. Juergen Schwemmer
  D-55122 Mainz, Canisiusstrasse 21
  Phone: +49 6131 18-0 (direct -2210)
  Fax: +49 / 61 31 / 18- 56 18
  Website: http://www.digitalesignatur.de

– Technical support agency:
Bundesamt fuer Sicherheit in der Informationstechnik (BSI)
Mr. Keus
D-55133 Bonn, Godesberger Allee 183,
Phone: +49 228 9582-0 (direct -141)
Fax: +49 / 228/ 9582-455

Greece

General

No related legislation has been enacted so far to amend, where appropriate, technology or media specific requirements in current laws or policies that may impede the use of information and communication technologies and electronic authentication mechanisms. However, Law 2472/97, on the protection of the individual with regard to personal data processing, sets out requirements for the processing of data (previous consent of the recipient, a certain security level during this process). The relevant Law prevents, and allows only exceptionally, the processing of "sensitive" data, for example, information referring to political ideas, race or ethnic origin. In this regard the unlimited use of information technologies as regards the processing of data may be prohibited unless the required conditions are met. As a general comment therefore, the provisions of Law 2472/97 are in accordance with the relevant articles (Art.10-13) of the 1996 UNCITRAL Model Law on Electronic Commerce. There is no specific law or regulation directly or indirectly related to any kind of electronic authentication to date. However, Art. 2 of Law 1805/88 adds a new paragraph to Art.13 of Greek Penal Code, and includes within the legal definition of the "document" "*any means that can be used by a computer in electronic, magnetic or any other way for the storage, record, production or reproduction of data as well as any other magnetic or electronic material in which any information intending to prove certain facts is entered*". Furthermore, Art. 14 of Law 2672/98 (within its limited applicability as is explained under question 5) defines the electronic signature as a form of electronic authentication, sets out the minimum requirements of an authentic digital signature and establishes the grounds for transfer of documents between administrative authorities and private parties through electronic mail. In addition, a presidential decree is currently being drafted, according to the proposal of a Commission Directive for electronic signatures (COM 1998, 98/0191 COD). Once adopted, it will regulate electronic authentication and in particular digital signatures. Greece does not recognise at the national or sub-national level any published criteria, and therefore electronic documents or signatures are not admissible for evidentiary purpose. In addition, no public or private sector body exists that issues digital certificates for public use in Greece. However, significant efforts have been made in this direction. Certain administrative authorities and public agencies, such as the Ministry of Finance, have begun to address the issue of digital certificates in the context of electronic submission and payment of VAT forms which has begun on an experimental basis. In addition, the Athens Chamber of Commerce and Industry (ACCI) has, since 1998, set up a pilot certification authority that is capable of issuing certificates to individuals and WWW servers.

Although the government does not use any authentication technologies or mechanisms in the electronic delivery of government services to citizens, the above mentioned Art. 14 of Law 2672/9 (which has a limited application to communication either within the public sector or between the public sector and

individuals, but excluding communication between individuals) sets out the minimum requirements for an authentic digital signature. The digital signature in order to be regarded as authentic must:

- Be related exclusively to the undersigned.
- Identify the undersigned.
- Be created through means that the undersigned can keep under his control.
- Be connected to the data to which it is referring in a way that the subsequent alteration of the relevant data will be prohibited.

The following legislative efforts are currently underway or under consideration in the area of authentication and certification; in the private sector that are no models in operation for electronic authentication:

- Article 14 of Law 2672/98 (concerning digital signature as a form of electronic authentication).
- Law 2472/97 (on the protection of the individual with regard to personal data processing).
- The draft presidential decree, pursuant to Council Directive 98/34 and to the Commission proposal 98/0191 (COD), which shall regulate the electronic authentication and the certification authorities.

An important development relates to the work of the National Committee of Electronic Commerce, established in 1997 by the Ministry of Development. Its main purpose is to reform the institutional framework in order to accelerate the development of electronic commerce in Greece. A working group from the Committee is currently reviewing all regulatory aspects of electronic commerce (its work is focused on issues relating to electronic signature, certification and authentication process, cryptography, validity of electronic messages). In 1999 it will propose legislative changes to the framework for electronic transactions. Moreover, scientific research sponsored by the official authorities is taking place in order to facilitate the use of the authentication and certification technologies by the public.

Private contractual agreements

Greece is awaiting specific related legislation on private contractual agreements concerning the use and recognition of digital signatures, electronic signatures, or other kinds of electronic authentication. No specific legislation exists regulating standards, procedures and uses that differ from those set forth in national laws and regulation. Therefore, the parties are free to agree to standards, procedures and techniques through the use of bilateral and multilateral interchange agreements. The problem, however, with such agreements is the enforceability (as a matter of essence as well as a practical matter) in a Court of Law. Concerning the application of evidentiary standards to evidence of validity and authenticity offered to a judicial or administrative proceeding, the Greek Civil Code in Art. 158 - 160 rules that the document, as a method of proof, must bear the handwritten signature of the issuer of the document. However, the legislator moves a step further and regulates in Art. 163 of the Civil Code that the imprinting of the signature by mechanical means has the same legal validity as the handwritten signature. Moreover, Art. 444-445 of the Civil Procedure Code defines that the representations by technical means are regarded as private documents with evidential effect. Pursuant to Art. 457 (para.4) of the Civil Procedure Code, the authenticity of such representations can be disputed before the Court of Law. In this regard, the Greek legislation accords evidential weight to representations produced by technical means. Greek civil law recognises the validity of agreements concerning the effect of certain type of evidence and parties are free to enter into such agreements. They are in a position to agree on the admissibility of

certain types of evidence and on the exclusion of others. Thus, the means of evidence which are not mentioned in the provisions of law can be used, should the parties agree. After relevant agreement, electronic records can have evidentiary value. An example is the electronic records of banks as far as overdraft amounts are concerned.

Technology requirements

As already stated, a national law or regulation relating directly to electronic authentication technology does not exist. However, as an indirect answer to the question regarding a law or regulation that specifically approves a particular kind of electronic authentication technology or mechanism, there are technology requirements in Law 2472/97 on the protection of the individual with regard to personal data processing. Art. 10 of the relevant Law sets out security requirements for the processing and the storage of the simple or "sensitive" data (for instance, the controller is obliged to take the appropriate organisational and technical measures for the security of the data and the processing of personal data is performed in secret). Moreover, the aforesaid draft presidential decree, which is under consideration and not yet enacted, will regulate the public and private key cryptographic system. Pursuant to Art. 3 of the relevant draft decree "The use of an asymmetric system is imperative for the security of the digital signature. This system will be based on a public and a private key which allows the signer, through the private key and the recipient, through the public key, respectively, to notify or to verify the digital signature".

Standards

No national or sub-national standards for electronic authentication have been developed by the public or private sectors in Greece. There are no laws, regulations or private sector mechanisms governing or developing/setting standards for digital signatures, electronics signatures, or other kinds of electronic authentication and compliance with any standards is not mandatory. Therefore, the failure to follow standards cannot, at present, give rise to liability in civil proceedings, nor increase the likelihood that a party will be held liable for the use of an alternative standard. However, in theory liability for not using standards could arise. An example could be the violation in the use of standards in the banking sector for funds transfer and for credit cards. So far, the private sector has not played a role in developing and certifying standards for digital signatures, electronic signatures, or other kinds of electronic authentication. Greek laws/regulations do not permit private-sector bodies to certify compliance with legislatively - or administratively - approved standards. However, the ACCI is running a pilot certification authority using digital signatures and is the only private sector initiative concerning standards and related issues in the area of authentication.

Certification authorities

Specific measures concerning the evaluation, approval and accreditation of certification authorities (or other providers of trusted services) have not been taken. However, the above-mentioned draft presidential decree defines that any authority that secures the validity of electronic documents can be appointed as a certification authority. Art. 3 of this draft sets out the conditions that have to be fulfilled in order to achieve this security. Several examples of these conditions are the accuracy of the information included in the recognised certificate, unless it is otherwise specified in the certificate, the reliable communication, the fast transfer of messages, the notification of the sending and receipt of the messages, the possibility of sending messages to the users at the same time and the possibility of international communication.

Currently, laws or regulations specifying the requirements that a certification authority must meet to operate in Greece have not been passed and no such private sector models exist. The following liability rules currently apply to the activities of certification authorities: pursuant to Art. 3 of this draft, the provider of the certification services shall have no liability for defective information, included in the certificate, provided that the certification authority can prove that all the appropriate measures for the verification of this information have been taken. Furthermore, the relevant certification authority shall have no liability for damages invoked by the irregular use of a recognised certificate which itself contains restrictions on its own use.

Global authentication

Greek law does not recognise digital signatures, electronic signatures, or other kinds of electronic authentication used in other countries. No related laws or regulations have been enacted so far to recognise foreign providers of trusted services related to digital signatures, electronic signatures, or other kinds of electronic authentication. No limitations have been placed on cross-border recognition of electronic authentication, nor have they been placed on cross-certification between certification authorities operating in Greece and certification authorities in other countries. No central public or private sector body exists that will cross-certify certification authorities at the national or sub-national level. At present, there are no private sector models in Greece for cross-certification authorities.

National contact points:

- Legal issues:
  Dr. Lilian Mitrou, Advisor to the Prime Minister
  E-mail: e.mitrou@primeminister.gr

- Government issues:
  Dr. George Papaconstantinou, Advisor to the Prime Minister
  E-mail: g.papaconstantinou@primeminister.gr

- General contact point:
  Data Protection Authority, attn. Mr. Loukeris
  E-mail: loukeris@otenet.gr

- Business contact point:
  Athens Chamber of Commerce and Industry, attn. Mr. Giannakopoulos
  E-mail: jvg@acci.gr

Iceland

Iceland has not yet set any laws or regulations on the use of electronic documents and digital signatures or set any other guidelines for certification. Work on legal barriers to electronic commerce and on digital signatures is underway.

National Contact Point

- The Ministry of Industry and Commerce
  Arnarhvoli
  150 Reykjavík
  Tel: 354-5609070
  Fax. 354-5621289

Ireland

Approach to Electronic Signatures

Ireland is fully committed to the development of a legal, regulatory and administrative framework which will facilitate the exploitation of electronic commerce. A key element of the measures being addressed by the Irish Government to promote electronic business is the establishment of a legal framework for the use of electronic signatures and the establishment of a system of nationally accredited certification authorities. Electronic signatures are designed to ensure the authenticity and non-refutability of electronic messages and are a key enabler in conferring on electronic communications the reliability and trust which now attaches to traditional written communications. Ireland's policy in relation to the use of electronic signatures is designed to promote the establishment of a legal framework that is conducive to the development of electronic commerce by providing confidence in the legal validity of electronic transactions and in the integrity of electronic signatures. It will be designed to provide for the use of digital signatures based on cryptographic techniques and for other forms of electronic authentication. The following are the principles on which the approach will be based:

- Legislation will be enacted to facilitate the use of electronic signatures through the establishment of a framework for the authorisation of bodies to act as nationally accredited Certification Authorities.

- Certification Authorities will issue certificates which verify the association between an individual or organisation and an electronic signature and Certification Authorities will be liable for the accuracy of such certificates.

- While it is recognised that the legal recognition of electronic signatures will ultimately be a matter for the courts, it is proposed to adopt legislation to minimise uncertainty as to the legal recognition of electronic signatures certified or issued by accredited Certification Authorities.

- The legislation will not prohibit, if the market so demands, the establishment of non-accredited Certification Authorities. The legal recognition of certificates issued by such authorities and any associated electronic signatures shall not be precluded.

- The regulatory requirements for accredited Certification Authorities shall ensure that they meet the highest applicable international standards (in terms of certification practice and electronic signature products) with the aim of ensuring that Ireland will be well placed to participate in any international framework for the mutual recognition of such systems that may emerge.

- Accredited Certification Authorities in Ireland will be obliged to implement mutual recognition agreements between each other.

- The regulatory framework shall be designed to cater for developments whereby new technological methods of ensuring the authenticity of electronic communications can be recognised by accredited Certification Authorities.

Italy

Italian Approach to Digital Signatures

Italy has been developing a national policy concerning cryptographic methods used to ensure legal effects of electronic documents for any purpose of law since 1995. The Italian Government approved, in September 1995, the Public Administration Unitary Network Project, which is intended to provide a communication network (as a result of the federation of the existing single public networks) between public agencies and citizens. The construction of this network infrastructure will be completed in 1998. This project could not be realised without citizens' trust and confidence in the legal value of the electronic documents and secure transfer of electronic payments between private entities and/or public agencies. For these reasons, the Italian Parliament and Government, taking into consideration the opinion of the Authority for Information Technology in Public Administration, enacted in 1997 a complete set of laws and regulations concerning the creation, storage and transmission of computer-based documents and digital signatures. The Italian law of 15 March 1997[14] declares that "[a]cts, data and documents created by public agencies and private persons by means of computer-based or telematic systems, contracts drawn up by such means, as well as their storage or transmission by means of computer systems, shall be legally valid and relevant for any purpose of law". The rules governing the implementation of the law principle by public agencies and private persons have been established in regulations enacted by presidential decree.[15]

Italian Technical Rules on Digital Signatures

A draft version of the Italian Technical Rules on Digital Signatures has been published[16]. The technical rules define the signature and hash algorithms to be used in three kinds of keys (signature keys, certification keys and time-stamp keys), the minimum length of the key as 1024 bit, the information to be contained in the certificates, the procedure to request a license as a CA, procedures for revocation and suspension of certificates, CA requirements (security measures, personnel, quality system), and time-stamping procedures.[17] The Technical Rules also adopt a licensing scheme for CAs). A CA may define

14. Law No.59 of 15 March 1997, "Delegation of power to the Council of Ministers to confer tasks and functions on Regions and local authorities, to pursue the reform of the public administration, and to simplify administrative procedures", published in *Supplemento Ordinario to Gazzetta Ufficiale*, N. 63 del 17 March 1997.

15. NR. 513 in November 1997 (published in Official Gazette NR. 60 of 1998). Text in English and Italian can be downloaded by the AIPA Web site at the address: http://www.aipa.it/english/law[2/index.asp.

16. See http://www.aipa.it/home/attivita/standard[5/firma[2/index.asp.

17. Articles I.2 and I.3, I.4, I.11, I.4, II.3, II.16-II.27, II.32-II.38, and III.1-III.11 respectively.

its obligations and limit its liability. If the legal effects of an electronic document last longer than the signature key, a time-stamp procedure has to be used.[18]

Authentication

The Italian regulation adopted the public key cryptosystem for digital signature purposes. Italian law makes a clear-cut distinction between using cryptographic systems for signing electronic documents or for data encryption purposes. The latter systems are not expressly considered in the regulations, since their scope of application and purposes are considered different from those related to document authentication. Italian legislation considers it essential that the total assent of the signatory on the content of the electronic document from a digital signature, as well as from a handwritten one should be able to be deduced. In contractual relations on open networks, digital signatures cannot be used only for identifying or authorising purposes, because verification of the integrity of data and of the identity of the sender does not necessarily prove the assent of the signatory on the content of the contract. For these reasons, a distinction should be made between authentication methods for identification purposes and "digital signatures", used by a signatory to indicate his approval of the content of data.

Certification

Certification operations in Italy are conducted by certifying authorities named in a public list accessible online. The list is created, maintained and updated by the Authority for Information Technologies (AIPA). Certifying authorities have to fulfil some technical and personnel requirements. If they are private entities, they have to be set up as *"società per azioni"* (usually equated to a public limited company, Joint Stock Company or Joint Corporation) and their registered capital must meet at least the working capital requirements for authorised banking enterprises. Legal representatives and administrators of certifying authorities must meet the requirements of good repute laid down for persons in executive, managerial or auditing positions in banks. Technical staff charged with carrying out certification procedures must be sufficiently knowledgeable and proficient to satisfy the provisions set out in the regulation and the technical rules established by Prime Minister's decree, having regard to the opinion of the AIPA Authority. Finally, the quality of computer-based processes and products must meet internationally recognised standards. The certification process may also be carried out by a certifying authority with a license or authorisation issued, subject to equivalent requirements, by another Member State of the European Union or European Economic Area. Any person or entity intending to make use of an asymmetric key or digital signature system shall take all necessary organisational and technical measures to prevent loss or damage to third parties. The CA must accurately identify the person applying for certification, issue and publish certificates and, on request of the subscriber, and with the assent of the third party concerned, specify any power of representation or other title relating to the subscriber's profession or office held. Exhaustive and clear information must be provided to the applicants concerning the certification practice and the technical requirements necessary to obtain certification. All certification procedures must comply with provisions concerning the minimal security standards of computer systems and the treatment of personal data.[19]

---

18. Articles II.3, II.32, and IV.1, respectively.

19. Law No.675 of 31 December 1996 concerning the protection of personal data.

Other Legal and Policy Issues

In Italy, CAs cannot accept the deposit of private keys. Electronic documents can replace conventional paper mail and Italian law applies a legal effect to electronic copies of conventional paper documents. The Law allows electronic documents and the digital signatures affixed or associated to the same documents, to be legally exchanged as a signed document, administrative act, or contract between private entities. The electronic records of the public administration, created by means of computer-based systems, are considered as original and primary information.[20] In all electronic files of Public Agencies, a digital signature shall substitute, in accordance with the regulation, for a required handwritten signature.

National Contact Point

– Dr. Giovanni Buonomo
Counselor at Law
AIPA (Authority for Information Technology in Public Administration)
Tel: +39 6 85 26 42 22
Fax: +39 6 85 26 42 51
E-mail: buonomo@aipa.it

Japan

Authentication policy

Japan's Information and Telecommunications Society Promotion Headquarters (chaired by the Prime Minister) established the "Working Group on Electronic Commerce" in September 1997 (chaired by Professor Nagaaki Ohama of Tokyo Institute of Technology). The Working Group was charged with developing basic concepts and clarifying major issues in the promotion of electronic commerce. The final report of the Working Group on Electronic Commerce was published on 18 June 1998.[21] In this report, electronic authentication is addressed as set forth in the following paragraphs.

- "Electronic authentication is used to verify the identity of a person with whom data is being exchanged electronically, and to verify that data has not been tampered with. It is a basic element necessary to ensure the security of electronic commerce. However, the required level of authentication and its function will vary according to the form of transaction.

- Various authentication methods and technologies are being rapidly developed, and electronic authentication issues are actively being discussed in the international community. Therefore, it is necessary to continue studying the authentication system in its entirety, with government involvement, ensuring that parties to transactions may freely choose the authentication method that best meets the requirements of the particular transaction format.

- As the disclosure of the information is required to judge the reliability of an electronic authentication system, self-regulation of the private sector with respect to the formulation of guidelines should be encouraged. The government of Japan is expected to promote the autonomous development of such

20. Section 18.

21. See http://www.kantei.go.jp/index-e.html.

electronic technology and guidelines. At the same time, the government is also expected to negotiate with foreign governments to ensure the regulations introduced in foreign countries are kept to a minimum and that they do not discriminate against authentication methods of other countries, since such regulations could become a barrier to the promotion of international electronic commerce. Furthermore, the government should also actively support attempts to establish impartial and neutral international standards for a secure electronic authentication system. The government is also expected to study the possibility of application of an electronic authentication system and electronic notary system which will be based on the current public administrative authentication services, including the commercial registration system.

- So called "electronic signatures" should at least be accorded the same legal status as handwritten signatures and seals. Thus, the Government should continue the research necessary to achieve this goal, including the clarification of basic rules regarding the rights and responsibilities of the parties to transactions. At the same time, it is required to take into consideration the compatibility of Japan's system with international efforts, for instance, the UNCITRAL preparatory work to draft a model law which has been under way since 1996."

The policy mentioned above was also stated in the US-Japan Joint Statement on Electronic Commerce.[22]

Private Sector Initiatives

In the Japanese private sector, a number of organisations are studying issues related to electronic commerce, including the Telecom Service Association of Japan, Cyber Business Association (CBA)[23] and the Electronic Commerce Promotion Council of Japan (ECOM)[24].

Related Initiatives

- Report on the Legal System of Electronic Commerce, Ministry of Justice (MOJ), Japan, March 1998.[25]

- Committee on the Improvement of the Environment for Electronic Commerce, Interim Report on Main Points, by the Ministry of International Trade and Industry (MITI), Japan[26].

- Study Group Report on Electronic Authentication, Ministry of Posts and Telecommunications (MPT), Japan, May 1997.[27]

22. See http://www.mofa.go.jp/policy/economy/e-commerce/statemt9805.html.

23. See http://www.fmmc.or.jp/index_english.html.

24. See http://www.ecom.or.jp/ecom_e/.

25. See http://www.moj.go.jp/ENGLISH/CIAB/ciab-17.htm (summary).

26. See http://www.ecom.or.jp/eng/miti/971127.

27. See http://www.mpt.go.jp/policyreports/english/group/Internet/elec-auth1.html.

- Guidelines for Transactions between Virtual Merchants and Consumers, Electronic Commerce Promotion Council of Japan (ECOM), March 1998.

- Certification Authority Guidelines, Electronic Commerce Promotion Council of Japan (ECOM), May 1998.

- Guidelines for Certification Authorities, Ministry of Posts and Telecommunications (MPT), Japan, May 1997.[28]

- Development of Internet Marks Technology for Authenticating Websites, Ministry of Posts and Telecommunications (MPT), Japan, 1998-1999.

- Cross-certification Guidelines, Electronic Commerce Promotion Council of Japan (ECOM), March 1998.

- Personal Authentication Technology Evaluation Criteria, Electronic Commerce Promotion Council of Japan (ECOM), March 1998.

- Electronic Notary System Guidelines, Electronic Commerce Promotion Council of Japan (ECOM), March 1998.

General

As there are no technology or media specific requirements in current laws or policies that may impede the use of information and communication technologies and electronic authentication mechanisms in Japan, no steps have been taken to amend technology or media specific requirements in current laws or policies. No specific law or regulation concerning digital signatures, electronic signatures, or other kinds of electronic authentication exists for the following reason. The principle of freedom of form of a contract in contract law, and the admissibility of all types of evidence in the Code of Civil Procedure, mean the present system is conducive to Electronic Commerce (EC). However, in addition, in an effort to ensure harmonisation with international organisations and other countries the question of which basic legal framework can be built is being examined. Furthermore, the establishment of a special standard that would render electronic documents or signatures admissible for evidentiary purposes is not required since in the Code of Civil Procedure, the admissibility of all types of evidence means that electronic documents and signatures etc. are naturally covered. It is expected that once a decision is made to use authentication technology that can confirm the identity of a person, public services will be offered in electronic form. The Ministry of Justice is currently establishing a certification authority based on the data in the commercial registry. This will allow certificates to be issued to representatives of companies registered in the commercial registry.

The following is a list of studies undertaken in the area of authentication and certification:

- Ministry of Justice (MOJ): “The report on The Legal System of Electronic Commerce” sponsored by the Director of the Civil Affairs Bureau. This was made public in April 1998.

28. See http://www.mpt.go.jp/policyreports/english/group/Internet/elec-auth2.html

- Ministry of International Trade and Industry (MITI): "Interim Report of Main Points". This was made public in November 1997. At the "Research Meeting for the Establishment of an Environment for EC", legal issues surrounding EC, including certification, were comprehensively considered, and a general direction was set. This year, in February, a study group for establishing the environment for EC was inaugurated. It is expected to investigate electronic signatures, certification, and consumer protection rules. In addition, in the 1998 fiscal year, in the first supplementary budget, 4.4 billion yen were allocated to projects for the development of certification technology.

- Ministry of Posts and Telecommunications (MPT): Policy issues on electronic authentication and its related areas were examined at the Study Group on Electronic Payment, Electronic Money and the Promotion of their Use (from November 1995 to April 1996) and the Study Group on Certification Authorities (from October 1996 to May 1997), and the final reports of both groups were made public. At the latter Study Group, the Guidelines on the operation of CAs (CA Guidelines) were prepared as a reference to help business in establishing its own certification policies. Taking into account recent developments, the Study Group on Cryptography for Communications was established in January 1999 to examine policy issues on cryptography as a fundamental technology for the information and communications sector, as well as those on electronic authentication as an important application of cryptography. In addition, the Telecom Services Association (TELESA), a private organisation supported by the MPT, is promoting a field trial of international electronic commerce using electronic authentication, and electronic commerce test-beds in Japan and Singapore have been interconnected since July 1998. In addition to being an officially registered APEC project, it has been highly regarded as an empirical pilot project for cross-border electronic authentication.

Finally, the ECOM is studying CA liability issues.

Several credit card companies and banks use Set compliant mode and private sector CAs issue certificates for business use.

Private contractual agreements

The principle of freedom of form of a contract is widely established. This is different from, for example, the Statute of Frauds, etc. in the U.S. In the first place, a handwritten signature is not required as a formal requirement to conclude a contract. Therefore, a contract concluded with an electronic signature has the same legal effect as one concluded with a handwritten signature. By the same token, parties are free to agree to standards and procedures as they wish. Parties may also use the national legal system to attempt to attain redress under the terms of the contract, since the legal system recognises the principle of freedom of form of a contract and the matter can be brought up as a matter of civil procedure. The admissibility of all types of evidence is enshrined in the Code of Civil Procedure, hence there are no formal requirements which limit evidentiary style. Moreover, the evaluation of evidentiary weight of evidence is left to the judge's free discretion.

Technology requirements

The legal foundations are currently being investigated regarding the use of an electronic authentication technology or mechanism that is not specifically approved. However, as a general opinion, we believe that the approval of only specific types of authentication technology, or of technical requirements for components or systems for electronic authentication, is inappropriate. The adoption of freedom of form of a contract and freedom of evidence evaluation means that there are no obstacles to the legal recognition of digital authentication techniques. Their recognition does not depend on specific laws.

Standards

Presently, the JIS standard dealing with entity certification, which is harmonised with international standards, establishes four criteria, mainly from the point of view of security. Japan believes this will promote the smooth development of EC. In addition, the MPT's CA guidelines, made public in May 1997, establish guidelines in privacy protection, operational management, and legal responsibility. Finally, ECOM is also establishing guidelines (certification guidelines, cross-certification guidelines, standards for certification technologies). The Minister of International Trade and Industry and the JIS Standards Body have regulations governing standards setting for digital signatures, electronic signatures, or other kinds of electronic authentication. According to Article 11 of the Industrial Standardisation law, the competent minister must, before establishing an industrial standard, consider the recommendations of the JIS. Alternatively, Article 17 states that established industrial standards can be made into JIS standards. ECOM is developing standards for digital signatures. JIS standards are optional ones, therefore standards related to certification are also optional. As JIS standards are optional, the outcome of civil proceedings concerning liability for failure to follow national standards is not always apparent. However, in the Code of Civil Procedure, the judge considers all the circumstances when evaluating the evidence to render the judgement. A decision to accept or reject the JIS standards on liability can form one of the elements in the decision. The following are private sector initiatives concerning standards and related issues in the area of authentication:

- CA Guidelines.
- Cross-Certification Guidelines.
- Evaluation Criteria for Personal Authentication Technology.

ECOM is also establishing guidelines for the above-mentioned issues.

Certification authorities

As a set of guidelines determining what conditions must be met for the management of a CA, the guidelines made public by the MPT offer a set of criteria to allow the evaluation of the level of trust of a CA. The following are private sector models for accreditation of certification authorities: Japan Verisign, Cybertrust, JCS, Entrust etc. The liability rules which govern the activities of certification authorities are governed by contractual agreements with users and general principles of civil law.

National Contact Point

- MITI: Electronics Policy Division, Machinery and Information Industries Bureau.
- MPT: Computer Communications Division, Telecommunications Bureau.
- MOJ: 4th Division, Civil Affairs Bureau.

Korea

Authentication and Certification

Korea has enacted the Digital Signature Act on 5 February 1999 and the Electronic Transactions Act on 8 February 1999. These Acts have regulations of electronic authentication and certification. Various electronic signature technologies are being used, and a digital signature algorithm adopted for national technical standards as a certification mechanism is used in the private sector. Digital certificates are used by some companies for identification of transacting parties. Korea is currently considering how business practice guidelines for entities issuing digital certificates can be improved, taking into account the ongoing evolution of commercial practices and technical standards. The Digital Signature Act recognises both identity certificates and authority certificates. The Electronic Transactions Act takes account of other technological developments in the electronic authentication area. Consideration is also being given to public key infrastructures and other architecture models for building trust in certification mechanisms. Various agencies and expert groups are developing plans, basic designs and policies relating to models for certification authorities and other mechanisms for building relationships of trust.

Legal and Policy Issues under Consideration

The Digital Signature Act and the Electronic Transactions Act were enacted to guarantee legal solutions for the use of digital signatures and authentication in electronic commerce. These laws have provisions to facilitate electronic commerce, including authentication, certification and authorisation of digital signatures. The Digital Signature Act applies to electronic authentication and certification services for all sectors, including private, commercial, governmental, and administrative transactions. The appropriate standards to ensure the integrity of data for electronic transactions and commerce, such as requirements for delivery assurance, time-stamp, and electronic storage, are considered in the context of the Act. Some laws which govern relationships with the government impose "quill and pen" requirements that specify that only written (or physical) signatures or seals must be used for "signing" a document. However, in general transaction laws, signatures or seals are not required, since the principle of freedom of contract applies. The general issues relating to electronic commerce are currently being addressed in agreements between transacting parties. The Electronic Transactions Act addresses the general issues related to electronic commerce at the level of the legal system. Issues such as how intent to sign can be established for electronic transactions are provided for in this Act. This Act adopts the 1996 UNCITRAL Model Law on Electronic Commerce to legalise the use of electronic signatures.

In terms of user protection, the Digital Signature Act contains provisions relating to privacy protection and the liability of a certification authority, and the Digital Signature Act requires certification authorities to ensure technical security, personal accountability and financial stability. Under the Digital Signature Act, a certification authority is liable for damages to a subscriber or a third party, which are caused

deliberately or by its fault, by reason of non-fulfilment of contract or unlawful action. A certification authority may establish limits on the use of certificates and the amount of money involved. The Digital Signature Act also defines criteria for a certification authority to be accredited. This Act requires an accredited certification authority to use digital signature technology based on the public key cryptography. The use of safe and credible authentication mechanisms is also a condition of accreditation. The Digital Signature Act sets limits to the use of certificates, but does not establish any limitation on the liability for damages. Under the Act, key certificates shall contain a time of expiration. According to the Act, the holder of a key certificate may request the certification authority to suspend a key certificate. From the Korean perspective, the main obstacles to the growth of authentication and certification services relate to the problems of protecting users (especially protection of privacy), cross-border recognition of digital signatures or certificates, unsettled technical standards, and controls on cryptography technologies. Korean national laws recognise all electronic transactions whether they originate from Korea or a foreign jurisdiction. According to the Digital Signature Act, Korea will provide cross-border recognition of digital signatures or certificates through mutual agreements with foreign governments.

Public Sector Approaches and Private Sector Initiatives

The Digital Signature Act and the Electronic Transactions Act are the main initiatives in the area of electronic authentication and certification in Korea. Internationally, Korea participates in the work of international organisations such as the OECD and UNCITRAL through which it hopes global agreement will be reached. Korea believes that OECD and UNCITRAL are the most important fora for discussing these issues.

National Contact Points

- Division of Information Security
  Ministry of Communication and Information of Korea
  Tel: 82 2 750 1260
  Fax: 82 2 750 1269

Mexico

Authentication

In Mexico, the company SeguriData has been developing cryptographic applications software and the central bank is working on the development and implementation of a public key infrastructure (PKI). The central bank will implement this PKI in the financial sector in order to facilitate the use of this technology by the commercial banks, and it will be open for use in other applications. Another company, InfoSel, is developing a certification network. In this network, public notaries will act as Certification Agents to legally identify people and to guarantee the ownership and confidentiality of private keys. This network will use the PKI developed by the central bank. In order to help electronic commerce flourish, and to promote competition in this field in an orderly manner, Mexico is developing a standard for defining digital certificates, and standard protocols for communication between different parts of the PKI.

Certification

Mexico has identified the needs of banks, state departments and service providers in terms of the provision and use of certification services in the electronic environment. It is also considering how business practice guidelines for entities issuing "digital" certificates can be developed. According to the Mexican approach, when authenticated and secure communication is required, public key cryptography must be used. If security and authentication do not matter, or if a lower level of confidence is acceptable for the transaction, then other methods can be used. Mexico believes that new regulations are only required for public key cryptography with Identity Certificates, and that other cases work under the present regulations. All certificates in the "Extended Security Infrastructure" will be Identity Certificates. In the case of legal persons, a natural person will own the Identity Certificate and use it under the authorisation of the legal person. The Mexican approach to electronic authentication and certification is neutral with regard to the underlying technology; a new technology is seen as basically a new way to use existing cryptographic methods. Any tests must be provided by the participants in the transaction and the computers used in the network. The Mexican policy in relation to public key infrastructures and other architecture models for building trust in certification mechanisms is to develop an Extended Security Infrastructure that will be open in terms of software development for the infrastructure. The authorities will be regulated by a central agency, authorised persons will run the agencies and any interested person (public or private sector) can use the system. The model in Mexico implements the certification process (legal identification of a natural person) with two different procedures. First, the person may be identified by a public notary and the certificate will have the highest level of security for user confidence. Second, the person may be identified by a certification agent (not a public notary); such a certificate will have a lower level of identification security. The public sector is considering the use of this system, and the first user is a part of the Mexican payment system.

Authentication, Certification and Related Services

The areas of potential application for authentication and certification services in Mexico include payment systems, central bank operations, commercial bank services, taxation and the public register. Regarding requirements for ensuring the integrity of data for electronic transactions and commerce, central bank regulations contain certain operational security mechanisms. In the near future, provisions about digital signatures will be incorporated. This regulation will require time stamping synchronised with the national time, and digital signatures or secure communication channels.

Legal and Policy Issues

Some Mexican laws impose "quill and pen" requirements that specify that only written (or physical) signatures or seals can satisfy legal requirements for "signing" a document. The method for establishing an "intent to sign" has not yet been specified in Mexico. A proposal currently under consideration is that the intention to sign will be implied where the user types his password phrase to permit the system to open his private key to digitally sign a document. To accommodate the provisions of the UNCITRAL Model Law on Electronic Commerce it would be necessary to make certain modifications to the Mexican Commercial Code. The Mexican delegate to UNCITRAL is currently preparing a draft for the modification of the Mexican codes to incorporate the Model Law. In principle, a certification authority must be authorised by a central agency, which is to be established in the near future. The reason for this authorisation is to develop an orderly infrastructure and to verify that the same definitions of certificates and algorithms are being used by all participants. Mexico considers that the activities of certification

authorities must carry some liability. One proposal for limiting the liability of certification authorities is to use the same mechanism as used by airline companies; that is, to fix a maximum limit to liability. Certification authorities will be liable for an error in the identification of the certificate owner. In the case of a disagreement, a certification authority has the means to demonstrate that its work has been performed properly. In terms of evaluating and approving certification authorities, the Mexican Government will require certification agents to be insured in order to guarantee their behaviour. Mexico will also demand technical and legal examinations of the authorities. There are currently no requirements in Mexico on the equipment used by a certification authority for accreditation.

There are two committees responsible for developing certificate policies and certification practice statements in Mexico: CCNN-T and Comité EDI-México. The mandate of the first committee is to create a NOM (*Norma Oficial Mexicana*) for information security. The second committee is developing standards for EDI including digital signatures. Regulations will be proposed in the near future to facilitate the development of a coherent PKI. The holder of a key certificate in Mexico may request the certification authority to bar the key certificate. The Extended Security Infrastructure will be capable of revoking certificates online, and informing participants of the status of any certificate online. It will also provide for the publication of revocation lists. A key certificate in Mexico must contain a time of expiration. Mexico is considering how global, seamless authentication and certification mechanisms should be developed. Where the same kind of technology is being used and both systems offer the same level of security and authentication, the problem can be solved by the interchange of the public keys of different systems in order to cross-check digital certificates. When the parties use different technologies offering different levels of security and authentication, the problem will be much more complicated. The Mexican Government believes that the main obstacle to the development of authentication and certification technologies in Mexico is the low number of home computers. It is likely that in the near future this technology will begin to spread in the industrial, financial, large commercial and public sectors and, in the end, it will reach the individual level. The government is working on different solutions to promote individual computer use. Mexican laws regulating the central bank, and other codes, contain provisions recognising electronic transactions. The Extended Security Infrastructure takes into account the cross-border recognition of certificates. The Infrastructure must be capable of storing foreign certificates and offering the same kind of services for these certificates as for national certificates.

Public Sector Approaches and Private Sector Initiatives

The major initiative underway in Mexico in the area of electronic authentication and certification is the creation of a Mexican Official Norm (NOM) for the structure of standard certificates and communication protocols for use between the different parts of the infrastructure. The inclusion of operational procedures into the norm is also being considered.

International Aspects

Mexico sees the OECD, APEC and UNCITRAL initiatives as the most important efforts aimed at examining the legal and policy aspects of authentication and certification. However, a discussion in an international technical fora is also valuable. Mexico believes it is necessary to first develop the technology and to take into account the different possible solutions to these problems. For example, it is necessary to take into account the notary systems being used before taking action or trying to resolve these issues.

General

Mexico is reviewing its commercial laws to include the UNICITRAL Model Law on Electronic Commerce. The Central Bank of Mexico (*Banco de México*) is developing a PKI to be used by the Financial System, and is monitoring the private sector that is developing a PKI in order to guarantee the development of an acceptable Public PKI. At present there does not exist any specific law or regulation concerning digital signatures, electronic signatures, or other kinds of electronic authentication. However, any kind of electronic signature can be used, the only requirement being to sign a contract between the parties. Following this, any system can be developed. A private sector body called Infosel is deploying a PKI; also the Central Bank is working in a PKI for the financial system and is looking for a national uniform PKI. It is possible that other organisations are working in similar schemes in Mexico at this moment, however, the government is unaware of other companies working in this area. The government is beginning to use authentication technologies in the electronic delivery of government services to citizens: SECOFI (*Secretaria de Comercio y Fomento Industrial*) is using a public key cryptosystem to implement a public registry. SECODAM (*Secretaria de la Contraloría*) is using a public key cryptosystem to implement its public buying system and SHCP (the Ministry of Finance) is using public key cryptography to receive tax declarations. The central bank is using this technology to protect payments in its high value payment system.

Activities currently underway in the area of authentication and certification include the National Consultative Committee for Telecommunications in Mexico, which is developing standards "NOM" (*Norma Oficial Méxicana*), which are compulsory standards for the use of the public key technology. The NOM 157 will deal with information security. The goal of this NOM is to define different levels of security for various uses, and to develop the appropriate language to describe electronic security in Mexico. In the private sector, a company called Infosel is developing its system "*Firma Electrónica*" which uses public key technology. *Banco de Mexico* is developing a system, which will use the concept of online verification, for real-time operations online. Both models are being developed using international standards. The government is beginning to use authentication technologies in the electronic delivery of government services to citizens. SECOFI (*Secretaria de Comercio y Fomento Industrial*) is using a public key cryptosystem to implement a public registry. SECODAM (*Secretaria de la Contraloría)* is using a public key cryptosystem to implement its public buying system and SHCP (the Ministry of Finance) is using public key cryptography to receive tax declarations. The central bank is using this technology to protect payments in its high value payment system.

Private contractual agreements

There are no Mexican Laws or Regulations related to regulation on private contractual agreements concerning the use and recognition of digital signatures, electronic signatures, or other kinds of electronic authentication. In general, parties are free to agree to standards, procedures, and uses that differ from those set forth in national laws and regulations. However, in the financial system, the corresponding authorities can enforce the use of certain standards to guarantee a desired level of security. As there are no evidentiary standards yet, they cannot be applied to evidence of validity and authenticity offered to a judicial or administrative proceeding.

Technology requirements

The National Consultative Committee for Telecommunications is at present working on the issues of approved electronic authentication technology, levels of security etc.

Standards

The Mexican Electronic Data Interchange Committee, EDI-Mexico, is using international standards where possible and has defined a protocol to deal with the problem of certificate verification to develop electronic transactions online. There are no laws, regulations or private sector mechanisms governing or developing/setting standards for digital signatures, electronic signatures, or other kinds of electronic authentication, but compliance with standards is mandatory under NOM 157. The private sector is co-operating with the government in the creation of national standards and has participated in the development of NOM 157. Mexican regulations do not permit private sector bodies to certify compliance with legislatively- or administratively-approved standards.

Certification authorities

NOM 157 is a measure designed to evaluate and approve certification authorities. No private sector models for the accreditation of certification authorities exist, and there is not as yet a mechanism to recognise private sector-accredited entities. At present, there are no proposals to limit the liability of certification authorities.

Global authentication

Mexican law recognises digital signatures, electronic signatures and other kinds of electronic authentication used in other countries, but for Telecommunications, the National Committee will discuss the details of the cross-border recognition later this year. There are no limitations on cross-border recognition of electronic authentication. There are no procedures to recognise foreign providers of trusted services related to digital signatures, electronic signatures and other kinds of electronic authentication and cross-certification procedures do not vary by sub-national jurisdiction. The Mexican Electronic Data Interchange Committee, EDI-Mexico, has developed a model that permits cross-border recognition of certificates. The CA must register its certificate in the local PKI in order to get a permit for the online certificate verification. Currently, no limitations are placed on cross-certification between certification authorities operating in Mexico and certification authorities in other countries.

National Contact Points

- Dra. Luz Alicia Fucugauchi
  E-mail: aliciaf@cft.gob.mx
- Oswaldo Tello
  Director for Commercial Development
  Ministry of Trade and Industrial Development
  Tel: (525) 229 6187
  Fax: (525) 229 9506
  E-mail: otello@secofi.gob.mx

– Raymundo Peralta
Information Technology Division Manager
Banco de Mexico (Central Bank)
Tel: (525) 227 8809
Fax: (525) 227 8759
E-mail: rperalta@banxico.org.mx

Netherlands

Several initiatives have been launched to stimulate the use of electronic commerce by generating confidence and trust in electronic communications for both consumers and businesses. An important initiative is the development of an interoperable infrastructure for trusted third parties (TTPs). Legal activities related to the use of electronic documents have also been initiated in the context of a government programme on competition, deregulation and legislative quality. A specific programme on legislation for the electronic highway has also been established.

Draft Proposal Concerning the Dutch Policy in the Field of Trusted Third Parties

In March 1998, the Dutch National TTP project was completed as part of the Dutch "National Action Program on the Electronic Highways", an initiative of all governmental departments. The TTP project was organised under the direction of the Ministry of Economic Affairs and the Ministry of Transport, Public Works and Water Management. It investigated the conditions that should be formulated for providing and using TTP services in the Netherlands. It also examined the way in which the formulated conditions can best be safeguarded. Furthermore, one of the goals of the project was to come to a well-considered development of a Dutch TTP infrastructure. It describes a market-driven certification scheme and a TTP Chamber to ensure that the requirements will be met. A draft Policy Proposal has been prepared but, pending the development of a policy view on the purpose of lawful access, it is still to be finalised. As the Dutch government is a large IT-user with a significant interest in the security of its own data and data exchange between governmental institutions, the private sector and citizens, it is currently studying its own needs and requirements for TTP services.

A Market Driven Project

On the basis of the draft Policy Proposal and international developments, a market-driven continuation and implementation project, called "TTP.NL" started in September 1998. Representatives of providers and users of certification and other TTP services participate. The aim of the project is to stimulate the development of secure and trusted methods for communicating and storing electronic information by developing a national, interoperable TTP infrastructure. It is designed to produce a close connection between the project results and the needs of market participants. In this project a Steering Group and three Working Groups have been formed with participants from business, consumers and government. The Steering Group is responsible for co-ordinating the overall project and decision-making. It is important that market participants (including providers and users of TTP services and intermediary organisations) participate in the working groups in order to reach a broad-based consensus. The three Working Groups will be responsible for the following activities:

- Drafting a Certificate Policy for the TTP infrastructure. Such a Certificate Policy will define requirements for a TTP to meet in order to operate in the Netherlands. The Certificate Policy will also address topics such as liability and the use of standards. The Working Group will adopt the conditions as formulated in the Draft Policy Proposal of the former National TTP project and will, if necessary, define additional conditions.

- Investigation of the institutional and operational aspects of a TTP Chamber. Preliminary talks indicate the need to establish an umbrella-organisation of TTPs. Other subjects for this Working Group are the management of the Certificate Policy and the subsets for the specific TTP services and the guarantee of the international interoperability.

- Defining and setting up an accreditation and certification scheme for TTPs in the Netherlands.

The project will run for one year. In that time it is expected that the necessary infrastructure and "tools" for the development of TTP services in the Netherlands will be completed. During the project all relevant market parties will be consulted and kept informed.

Apart from this initiative, the Netherlands recognises that a number of individual organisations and companies are trying to establish themselves as TTPs. Among these are public notaries, national post organisations (secure e-mail) and banking institutions. All of these organisations are taking part in the TTP implementation project discussed above.

Code of Conduct for Electronic Commerce

Another Dutch initiative related to trust and confidence is the project on self-regulation in electronic commerce. In the context of the Dutch action on electronic commerce, EDIFORUM (the national EDI umbrella organisation) and the Electronic Commerce Platform in the Netherlands, a convention was held in June 1998 at the request of the Ministry of Economic Affairs. The key issue which was put to representatives of relevant market players such as ministerial departments, banks, universities and large businesses was: “Legal framework governing electronic commerce: Self-regulation?” It was agreed that self-regulation can make a positive contribution in fostering trust in electronic commerce owing to the speed with which a Code of Conduct could be prepared, the flexibility of self-regulation and the strong supporting platform which may be implemented by self-regulation. The points that the market participants would like to have included in a Code of Conduct were identified. Some examples are: electronic agreements, reliability, confidential information, proof and data storage, jurisdiction and the applicable legal system. A start can now be made on preparing a draft Code that became available in April 1999. The final Code of Conduct on Electronic Commerce will be presented at the end of 1999 following another broad-based consultation process in which all relevant market players will be invited to comment.

Initiatives Fostering Electronic Signatures

In Dutch law there are no formal requirements for most contracts. This means that parties are free to decide in which way their contracts are concluded (orally, in writing, with the presence of witnesses etc.). If a dispute arises between the parties concerning the contract, they can go to court, where they are free to present evidence as to the existence of the contract and its content, and the judge will decide whether the evidence offered is acceptable or not. There are, however, some contracts and legal acts that are only

valid if put in writing or if they meet other formal requirements (such as preparation by a public notary or the presence of witnesses). In the context of the Dutch Government project on competition, deregulation and legislative quality a working group has studied the possibility of electronic contracts and entering into legal acts for which Dutch law presently specifies formal requirements. It appears that the electronic techniques being used cannot equal the legal guarantees offered by the formal requirements. Therefore the working group has developed a number of conditions that must be fulfilled if a legal document is drawn up electronically in order to offer the same protection and guarantees as the actual formal requirements. The Council of Ministers agreed on the proposals in April 1998. On the basis of the recommendations, the Dutch government has decided to introduce new legislation. Proposals will concern administrative law and civil law. In administrative law, it will be possible for citizens to use electronic means in administrative proceedings (for example, the application for a construction permit) and also for the authorities to inform citizens of their decisions by electronic means. In the Dutch Civil Code, regulations will be introduced to facilitate electronic transactions. New legislation will be proposed that will make it possible to make use of electronic means in transactions concerning the buying/selling of real estate. Furthermore, the working group has recommended self-regulation by the market and experimental legislation. In order to stimulate self-regulation, a new business-government expert group has been created in which public authorities and the various market representatives participate.

Legislation for the Electronic Highways

The use of electronic signatures is one of the topics in an overall policy paper by the Dutch Government, entitled “Legislation for the Electronic Highways”. In this policy document, which was approved by the Council of Ministers in February 1998 and is currently the subject of parliamentary discussion, the Dutch Government presents its opinion on the effects of the information society on the Dutch legal system. Future government action will be based on this policy document. The policy document concludes that the existing legal framework is generally applicable to the electronic highway (after amendment where necessary). An important qualification is, however, that the international nature of the electronic highway does not fit easily with territorially organised government, as physical barriers are not a factor in the electronic highway. The policy document concludes that there is no all-embracing solution to this problem, although it can be substantially reduced by a combination of solutions. To this end, the policy document proposes a pragmatic multi-track approach, on the basis of existing national sovereignties. An important point for the Dutch government is that the same rules that apply in the physical world (“off line”) should apply “online”. Technology-independent legislation is preferred. In many cases, this achieves equivalence between the off-line and the online world and may also be better equipped to deal with technological turbulence. In some cases, however, technology-dependence is required. The need for legal certainty could, for example, create a need for technology-dependent legislation. In the short term, self-regulation is preferred but also entails risks. The preference for self-regulation does not apply where fundamental values and standards of the constitutional democracy are at issue. Another preference is, of course, that international solutions prevail over national solutions. The policy document provides concrete legislative proposals, aiming, amongst other goals, to create a reliable infrastructure for electronic commerce and, on the other hand, to meet the reasonable interests of law enforcement authorities.

General

The Netherlands does not recognise published criteria, the observance of which renders electronic documents or signatures admissible for evidentiary purposes. However, the Netherlands does recognise

criteria from the Code of Information Security, which is in line with British Standard 7799, the PKIX and the EU directive on electronic signatures for quality evaluation of organisations that produce TTP services. A private sector body exists that issues digital certificates. This is the former public post organisation PTT Post that offers a service called 'Keymail'. It includes both Certification Authority (CA) and Registration Authority (RA) services. Although authentication technologies are not used in the electronic delivery of government services to citizens at present, initiatives have been started to use them. Currently underway is a joint initiative of both the public and private sectors called TTP.NL that aims to stimulate the creation of a voluntary certification system. Concerning private sector models for electronic authentication, there is the Keymail service, mentioned above, which is in operation. Authentication takes place through postmen visiting home locations.

Private contractual agreements

There is no law or regulation on private contractual agreements concerning digital/electronic signatures and therefore parties are free to agree standards and procedures as they wish. Similarly, the parties may use the national legal system to attain redress under the terms of the contract since they would not be in breach of national regulations as they do not exist. Compliance with criteria set in TTP.NL, including criteria from the EC directive on electronic signatures assists in forming evidence of validity of authenticity offered to judicial or administrative proceeding. However, this compliance does not have to be sufficient for forming evidence.

Standards

There are presently no national or sub-national standards for electronic authentication but a national procedure for electronic authentication is in the process of being developed jointly by the private and public sectors in the project TTP.NL. This standard is derived from the PKIX standard that is used as the framework for the standard. Other existing standards, like British Standard 7799, the EU directive on electronic signatures and the requirements of the draft national policy paper on Trusted Third Parties are taken up in this framework. A joint public and private sector initiative, the project TTP.NL, exists, which is developing standards for digital/electronic signatures, and is also concerned with standards in the area of authentication. Through TTP.NL, it is intended that private organisations will be able to certify compliance with legislatively- or administratively-approved standards. Compliance with any standards is currently not mandatory as TTP.NL is based on a voluntary certification system. Liability for failure to follow standards mainly depends on the content of clauses (Certificate Practice Statements) made by Trusted Third Parties. Furthermore, there is a system of free evidence so that liability can not *a priori* be determined.

Certification Authorities

Standardisation of the process and criteria for the evaluation and approval or accreditation of certification authorities is being investigated in the TTP.NL project. No requirements are set for licensing or accrediting "certification authorities" through laws or regulations. A private sector model for accreditation of certification authorities (the project TTP.NL), is under development. The requirements that a certification authority should meet are in the areas of:

- Reliability of the technology used, personnel, finance and control.
- Quality of administration and clarity of rules with respect to liability.

- Privacy related issues, such as high confidentiality through secure techniques, and privacy policy statements.
- Interoperability of the operational process.
- Legal access.
- Independence, both financially and with respect to other market parties.

There are no laws or regulations that have mechanisms to recognise private sector-accredited companies and the requirements for licensing or accrediting "certification authorities" do not vary by sub-national jurisdiction. The normal rules from the Civil Code with respect to liability currently apply to the activities of certification authorities. This means that there are no limitations to their liabilities. Certification authorities that exclude all liabilities in their Certificate Practice Statements can in jurisdiction still be held liable. At present there are no proposals to limit the liability of certification authorities, but is under investigation in the TTP.NL project. Furthermore, the implementation of the EU directive on electronic signatures can be of interest.

Global authentication

In the Netherlands, there is a system of free evidence so that in addition to digital/electronic signatures, additional evidence may be necessary in case of a dispute in court. There are no procedures to recognise foreign providers of trusted services. There is freedom to make use of such services, and a system of cross-certification, based on auditing against own criteria, is used for foreign organisations in order to reach an equal status of domestic certification authorities. In addition, there are no laws or regulations that place limitations on cross-border recognition of electronic authentication or on cross-certification between certification authorities operating in the Netherlands and certification authorities in other countries. At present there is no central private or public sector body that cross-certifies certification authorities. However, such a body is being developed (TTP Kamer). This organisation would operate at the national level and cross-certification procedures would not vary by sub-national jurisdiction. However, there is a private sector model for cross-certification of certification authorities, embodied in the project TTP.NL.

National Contact Points

- R.M. van der Luit
  Ministry of Transport, Public Works and Water Management
  Directorate-General for Telecommunications and Post
  P.O. Box 20901
  2500 EX The Hague
  Netherlands
  Tel: +31 70 3517793
  Fax: +31 70 3516366
  E-mail: ronald.vdluit@dgtp.minvenw.nl

New Zealand

In New Zealand, the role of policy development for the general area of public key cryptography, including authentication and certification issues, lies with the interdepartmental National Cryptography Policy

Committee. The Government Communications Security Bureau (GCSB) has conducted a pilot of a New Zealand public key infrastructure (PKI) for the government sector. While some individual departmental initiatives are underway, plans for a government-wide implementation have yet to be confirmed. There are no agencies currently addressing the requirement for PKIs outside government. There is at least one private sector certification authority preparing to begin operations in New Zealand in the near future. Two major studies have been conducted; the New Zealand PKI pilot conducted by GCSB noted above and a study of the legal implications of electronic commerce conducted by the New Zealand Law Commission.[29] In its draft report the latter concludes that "there are no legal difficulties in authentication which are unique to electronic documents" and also concludes that New Zealand should follow the principles of the UNCITRAL Model Law on Electronic Commerce, with emphasis on the need for technological neutrality and minimalist legal intervention. A strength of New Zealand law is that it is principle-based and in general does not differentiate between electronic commerce and paper-based commerce, or between different technologies. Should the recommendations of the draft report of the New Zealand Law Commission be followed, it is unlikely that specific legislation on electronic commerce will be developed. However, some changes may be made to existing legislation to confirm and provide a level of assurance that current law is applicable to electronic as well as paper-based commerce.

General

The New Zealand Law Commission will provide advice to Government later this year concerning the use of information and communication technologies and electronic authentication mechanisms. In general, New Zealand law aims to be independent of technology and it is believed that digital signatures are probably covered under existing law. Nevertheless, it is recognised that there may be a need to clarify the position by amendment to the existing statutes. Information is collated by the New Zealand Law Commission in *Report 50: Electronic Commerce Part One: a guide for the legal and business community* (September 1998). http://www.lawcom.govt.nz/pub_index.html. At this stage there is only one private sector agency that issues digital certificates for public use but other groups are looking at this. The agency is a private registered company, 128i Limited, Wellington, New Zealand. The Inland Revenue Department has issued digital certificates to over 12 000 employers responsible for PAYE (income tax) payments. As of 1 April 1999, employers are required to make tax returns using the certificates unless they have an exemption, which is available in certain cases for up to 12 months. There are no initiatives, studies, proposed legislation or rules, or other activities currently underway or under consideration -- in the public or private sectors -- in the area of authentication and certification. Furthermore, there are no private sector models for electronic authentication that are in operation or under development.

Private contractual agreements

It is believed that New Zealand case law precedents would allow for electronic authentication of private contractual agreements. However, legislation may be required to provide greater certainty. This matter is currently under review (see reference to the Law Commission). Parties are free to agree to standards and procedures and may use the national legal system to attempt to attain redress under the terms of the contract. Evidentiary standards are discussed extensively in the New Zealand Law Commission report Chapter 5. In addition, the Commission will publish in June a major report outlining a new evidence code for New Zealand, including documentary evidence which also includes electronic documents.

29. This report will soon be available at http://www.lawcom.govt.nz.

Certification authorities

A Government/Private Sector group has been formed to look at what measures may be required for the evaluation, approval or accreditation of certification authorities. At present, the law does not govern or set requirements for licensing or accrediting "certification authorities" (or other providers of trusted services), nor are there any private sector models for the accreditation of certification authorities. Normal commercial contractual obligations apply to the activities of certification authorities and at present, there are no proposals to limit liability.

Global authentication

All questions in this section are covered by the comment that it is unlikely that there will be any discrimination under New Zealand law against, or specifically favouring, overseas certification authorities. Recognition of cross border certificates will be one consideration taken into account by the Study Group.

National Contact Points

- Frank March
  Specialist Advisor, IT Policy Group, Ministry of Commerce
  E-mail: frank.march@moc.govt.nz

Norway

In a government policy paper from 1996, on the development of the information society, it is clearly stated that electronic communication and transactions should be as valid as paper-based communications and other traditional forms of communications. At present the situation in Norway can be characterised by preparatory work, pilot projects and a few products on the market. Recently, policy formation processes have gathered speed.

Legal Issues

Some years ago certain amendments to the Customs Act, the Maritime Act and the Privacy Act were adapted to cope with the electronic environment. Recently, the Ministry of Justice has considered legal questions that recommended that laws and regulations that may impede electronic commerce should be identified. A survey of Norwegian laws and regulations is in progress, intending to identify obstacles especially form requirements to electronic communication, including electronic commerce and authentication. The European Union's proposal for a Directive on a community framework for electronic signatures is at present being considered for incorporation into the European Economic Area (EEA) Agreement and implementation in Norwegian legislation.

Studies and Reports

A recent report prepared by the Norwegian Government Council for IT Security emphasises the need to establish a clear legal regime and other necessary frame conditions for electronic signatures and

communications in general as well as for appertaining services, especially TTP services. The recommendations in the report include three types of measures, regarding (i) clarification of legal issues, (ii) further studies on digital signatures and TTP activities, and in this regard arrangements for voluntary accreditation, mutual recognition of certificates and types of roles in the market, and (iii) gaining knowledge and experience, for example by pilot projects. A study elaborating on item (ii) is now in progress, in relation to the European Union draft proposal on electronic signatures. As part of the Public Administration Network Project [30], the Ministry of Labour and Government Administration has specified requirements which are used in calls for tenders for TTP and digital signature services in the public administration.

Pilots and Products

There are a few Norwegian products on digital signatures on the market. "Postsek" of Telenor Conax[31] is currently available in a basic version that does not use certificates. Integration with certificates was planned for 1998. "SecApp" of Posten SDS[32], is available in several configurations, mainly with the use of Smartcards with strong encryption keys and certification procedures involving personal identification. The application fetches certificates and revocation lists in a full PKI manner from a public catalogue also administered by Posten SDS as the Certification Authority. Norway Post as the TTP also makes available a secure module (LRA) which is connected online to the Certification Authority but located in the user organisation for the distribution of certificate carriers (Smartcards) and PIN codes. Integration with browser technology is accomplished. The co-operation between the postal agencies in Norway, Sweden, Finland, Denmark and Ireland implies that certificates from these agencies are issued by cross-certified service providers. At present the names in the national catalogues are not fully transparent. This co-operation is brought forward in Universal Post Union (UPU) which is developing a Certificate Practice Statement with the intention that postal agencies which satisfy certain security profiles can mutually recognise their certificates.

General

A white paper to the Parliament on electronic commerce (June 1999) mentions *inter alia* a Government decision to produce an inventory of current laws and regulations that may impede the use of information and communication technologies. Special focus is on form requirements. The inventory is made sector by sector. Each Ministry shall submit a report to the Ministry of Trade and Industry before 30 September 1999. The reports will also contain opinions on whether laws and regulations that impede the use of information and communication technologies need to be amended or whether it is sufficient to change governmental practice or make other changes. The reports will be evaluated and recommendations put forward on how to implement amendments. The amendments shall enter into force before 1 January 2001. The issue of regulating electronic signature and trusted third parties etc. will also be addressed in this work. The Ministry of Justice has also drafted a "formal statement" on the possibility under current law to enter into agreements by using electronic communication. In addition, the statement concerns the

[30] See http://forvaltningsnett.dep.no

[31] See http://www.conax.com

[32] See http://www.sds.no/produkt/

evidential value of such an agreement – vis-à-vis a paper document with the same content - when produced before a court of law. However, it should be mentioned that the Norwegian Conclusion of Agreements Act (31 May 1918 - (4)) does not include specific requirements as to form and thus recognises in general the validity of electronic agreements. Furthermore, specific areas already have several acts that explicitly accept electronic communication, e.g. the Customs Act, the Archive Act and the proposed Act on Financial Agreement and Transaction Orders, coming into effect 1 July 2000.

There are no specific laws or regulations concerning digital signatures, electronic signatures, or other kinds of electronic authentication. In Norway, as in the other Nordic countries, the parties are free to present any kind of evidence to the courts and the courts are free in their evaluation of the evidence. This means that electronic documents (including contracts) with or without electronic signatures, are admissible as evidence, and their credibility will be assessed by the courts. Norway plans to implement the up-coming EU directive on a "community framework for electronic signatures". To prepare for implementation, work has been initiated to draft an act concerning electronic signatures.

There are several organisations that issue digital certificates in Norway. Some of them are major banks (Den norske Bank, Kreditkassen), using the certificates for secure fund transfer between banking institutions. Others include the Norwegian National Insurance Administration, issuing certificates for the purpose of secure exchange of EDI-messages from doctors and clinics applying for reimbursement. Then there are commercial companies issuing digital certificates for general purposes. These are: Telenor ASA, Posten SDS AS, Fellesdata AS and Merkantildata AS. One of those companies is being used by Norwegian taxation authorities to run trials for electronic filing of tax returns from private companies. The same company has participated in a trial exchange of documents, between a ministry and its agency, that were digitally signed and encrypted, involving the use of digital certificates.

The Ministry of Labour and Government Administration has established framework contracts with several of the above-mentioned companies, as well as some software companies that provide digital signature software solutions. The purpose of these contracts is to secure a quality offer of certification services for public sector organisations. The agreements are concluded. It is voluntary for the public organisations to call on the agreement but they will have to pay for the services and products provided. In general, there are many agencies, both on the central and local government level, that plan for electronic service delivery to citizens. Some local authorities have started trials for electronic application forms for benefits etc. on the Internet. What they will need to carry out the full potential of such services is a secure authentication method. By establishing the framework agreement, it is hoped that these mechanisms will now be available for the public sector to use. However, it remains to be seen to what extent the contracted services and products will be used during the agreement's duration period of one year.

The Public Sector Network Project, under which the framework agreements on TTP services and digital signature products are being established, is also a "test bed" for relevant legal, technical and organisational issues of a PKI. It is the intention of the project to sign agreements with several companies providing certification services, given that they qualify. One of the requirements under the contract will be to cross-certify the services of the other selected companies, so that the public bodies that want to use one of the companies will be free to choose any of them, not risking incompatibility with their possible communication partners. Cross-certification is still not solved, but will be discussed and solved in a special forum of TTP service suppliers. Another issue that is being sorted out under the project is the question of certificate content, especially with the view to unique identification of individuals and organisations. This involves the question of naming rules and naming authorities as well. The known models for electronic authentication are the previously mentioned digital certificates for secure funds

transfer as well as the oil industry's trial use of digital signatures for document exchange on their unified data network (the SOIL-project). The Norwegian Bank Clearance Institution (BBS) is also working on a digital certificate scheme in order to offer solutions for banks providing electronic banking services to their customers.

Private contractual agreements

In business-to-business relations the parties are more or less free to use standards etc, that differ from those set forth in national law and regulations. However, in a relation between a business and a consumer it is forbidden to depart from certain acts or provisions of acts if such action would be of detriment to the consumer. In the case of business-to-business electronic commerce, the parties may use the national legal system to attempt to attain redress under the terms of the contract, but the court may set unreasonable agreements aside. For business-to-consumer electronic commerce, the same applies but an agreement that sets aside mandatory regulations may also be set aside by the court.

Standards

Compliance with standards is not mandatory. However, the Public Sector Network Project has developed a standard requirements specification for TTP services and digital signature (and message encryption) products and services. The specification contains both user-oriented and technical requirements that encompass certification services, time-stamping services, verification services, digital signature and encryption software (and hardware), as well as smart cards and card readers. This standard specification is the basis for the establishment of framework contracts for the public sector and it is based on the SEIS-standards S1, S3 and S10. SEIS (Secure Electronic Information in the Society) is a Swedish interest group consisting of public and private organisations and vendors. They developed, amongst others, the publicly available specifications (PAS) for electronic ID-cards (smart cards holding identification data as well as digital signature, encryption and authentication keys). These specifications – S1 and S3, have also been adopted as Swedish national standards. The SEIS specification S10 is a model certificate policy for ID-cards and it is also being used in the Norwegian standard requirements specification for the public sector. We believe that requiring a common certificate policy will ease the question of cross-certification. The Norwegian national standards bodies plan to consider the SEIS-based Swedish standards for possible adoption as Norwegian national standards. In the Public Sector Network Project, emphasis has been laid upon a continuous dialogue with the vendor community, in order to arrive at commonly agreed standard requirements for TTP services and digital signature products. The requirements specification has been developed in an open process, with early drafts being published on the project's Website and available for all vendors and other interested parties, to comment upon and make contributions. Thus, the vendor community and the private sector have had an opportunity to participate in the development of PKI-standards for the public sector. Some of the vendors have used that opportunity quite well, with mutual benefit to the specification makers and the vendor companies.

Certification authorities

At present, in the field of authentication and certification, there are no laws or regulations that govern or set requirements for licensing or accrediting "certification authorities" (or other providers of trusted services), nor are there private sector models for the accreditation of certification authorities. When establishing the framework agreements for TTP services, the Ministry of Labour and Government Administration developed a model contract for TTP services that also addresses the liabilities of

certification service providers. There is a proposal on upper limits for the liabilities. Arrangements or schemes for evaluation and accreditation of certification authorities will shortly be evaluated by the Ministry of Trade and Industry (see section 132).

Global authentication

Digital signatures, electronic signatures, or other kinds of electronic authentication used in other countries are recognised in Norway since the parties are free to present any kind of evidence to the courts and the courts are free in their evaluation of the evidence. No limitations are placed on cross-border recognition of electronic authentication or on cross-certification between certification authorities operating in Norway and certification authorities in other countries. The Ministry of Labour and Government Administration will co-ordinate cross-certification of selected certification service providers that will come under the framework contract for the public sector. If a nationally designated body is established, responsibility for cross certification will be transferred to this body.

National Contact Points

– Legal issues:
Karin Fløistad
Ministry of Justice
E-mail: karin.floistad@jd.dep.telemax.no

– Thomas Aalby-Myhr
Ministry of Trade and Industry
E-mail: thomas.aalby-myhr@nhd.dep.telemax.no

Government issues:
- Katarina de Brisis
Ministry of Labour and Government Administration
E-mail: katarina.de-brisis@aad.dep.telemax.no

General contact point:
Jens Nørve, Ministry of Trade and Industry
E-mail: jens.norve@nhd.dep.telemax.no

Poland

General

Following upon the October 1998 *Ministerial Declaration on Authentication for Electronic Commerce*, the knowledge about the need to change the Polish legal regulation has increased. Poland is in contact with the UNCITRAL, and the Model Law on Electronic Commerce of 1996 is taken into consideration in the agreements between the parties that interchange electronic documents. Early this year work started to

prepare the necessary changes in the Polish law. The first results are expected at the end of 1999. Poland does not have a specific law concerning digital signatures. The legal regulation concerning electronic signatures in Poland for the whole country is being prepared. The specific regulation for the banking sector is being completed by the Polish Banking Association. Poland does not recognise at a national or sub-national level the published criteria that render electronic documents or signatures admissible for evidentiary purposes. There is no public body that issues digital certificates for public use. However, there is a private sector body that issues digital certificates for specific systems only. The Polish government does not use authentication technologies or mechanisms in the electronic delivery of government services to citizens.

Private contractual agreements

Polish law and regulations recognise private contractual agreements as the most important of all, and so recognise digital signatures, electronic signatures, and other kinds of electronic authentication. Parties are free to agree standards and procedures, and if they have cause to attempt to attain redress under the terms of the contract, a form of arbitrage is used. Evidentiary standards do not apply to evidence of validity and authenticity offered to a judicial or administrative proceeding in Poland.

Standards

The national standards for electronic authentication are now being chosen. There are no legal regulations on developing standards for digital signatures, electronic signatures, or other kinds of electronic authentication. The sector mechanisms develop standards for the needs of a particular sector. Compliance with standards is not mandatory, and so it is unlikely that a party will be held responsible for the use of an alternative standard. The private sector is ready to sell the certification service and the standards will be chosen according to the needs of the market and the law in the future. To date, Polish law does not permit private-sector bodies to certify compliance with legislatively- or administratively-approved standards. At present, only the banking sector is working on the standard of authentication.

Certification authorities

Poland is now preparing a Public Key Infrastructure, but the project is not yet completed. The question of accrediting “certification authorities” is currently under discussion. The private sector models are too individual to be a model for the whole sector or for the whole country.

Global authentication

Polish law does not yet recognise digital signatures, electronic signatures or other kinds of electronic authentication used in other countries, nor does it recognise foreign providers of trusted services related to electronic authentication. Polish law is not ready for cross-border recognition of electronic authentication and it also has not yet placed limitations on cross-certification between certification authorities operating in Poland and certification authorities in other countries. There are plans for a body that will cross-certify certification authorities at a national or sub-national level and private-sector models for cross-certification of certification authorities are also being examined.

National Contact Points

- Katarzyna Gonera
  Judge of the Court of Appeals in Warsaw
  Secretary to the Commission for the Codification of Civil Law
  Al. Ujazdowskie 11
  00-950 Warsaw, Poland
  PO Box 33
  Tel: +48 22 628 13 83

- Prof. Dr Zbigniew Radwanski
  Chairman
  Commission for the Codification of Civil Law
  Al. Ujazdowskie 11
  00-950 Warsaw
  PO Box 33
  Tel: +48 22 628 13 83

Spain

The use of an electronic means for administrative procedures in Spain is fostered by Administrative Law (*Ley de Régimen Jurídico/Procedimiento Administrativo Común*). Authentication for administrative procedures has been further developed by Royal Decree nº 263/96. Law 66/97 foresees that the *Fábrica Nacional de Moneda y Timbre* (MINT) will provide the security services for authentication and that the Postal Office will act as a registration authority. There is no restriction on the use of electronic devices for private purposes in Spain. In particular, there is no restriction on the use of cryptography.

Sweden

Authentication

In Sweden, to establish identity in digitally "signed" documents, registered individuals are assigned a personal ID-number (10 digits) and registered organisations are assigned an organisational ID-number (10 digits). This system is well established in both the public and private sectors. The ID-numbers are not used generally for establishing identity in the electronic environment. There is no general legislation in place aimed at helping electronic commerce flourish through the use of electronic authentication. There is, however, application-oriented legislation in the public sector relating to, for example, customs and taxation. The Swedish Government initiatives relative to authentication technology have focused on legal issues. The development of technical standards is being left to market actors. The goal of Swedish industry is to have standards that can be used internationally. The Secured Electronic Information in Society[30] Association (SEIS) is active in compiling and presenting requirements from industry and individual users.

30. See http://www.seis.se

Certification

Sweden has identified the needs of the various parties which both provide and use certification services in the electronic environment as part of the Government action to find solutions for the use of digital signatures. Real applications of "digital" certificates currently include use by some banks, the Swedish Post, and internal applications in large governmental and private bodies. Business practice guidelines for issuing "digital" certificates have been developed in the private sector by some banks, Swedish Post, and Telia, and for applications in governmental bodies. The ongoing evolution of commercial practices and technical standards development -- which are extending the use of existing technologies and practices toward new applications for "certifying" various kinds of information online -- are reflected in public policy discussions in Sweden. No regulations exist which prevent or support the recognition of certificates by Swedish national law. To take account of further technological developments in this area, the Swedish Government actively participates in the EU Council Working Group on electronic signatures with the goal of finding a common EU position. This position will form a basis for legislation in Sweden. Sweden has not currently adopted a policy in the area of public key infrastructures and other architecture models for building trust in certification mechanisms. In terms of the various options for public policy and technology architecture models for certification authorities Sweden has developed various pilot projects. Related legal issues are being studied in connection with on-going EU-consultation.

Authentication, Certification and Related Services

The areas of potential application for authentication and certification services include administrative, governmental, private commercial transactions, and consumer transactions. There are currently no legal requirements in Sweden for ensuring the integrity of data for electronic transactions and commerce (except for privacy protection). It is likely that such requirements will be introduced in the future.

Legal and Policy Issues under Consideration

There are many provisions in Swedish law relating to the public sector which specify that only written (or physical) signatures can satisfy legal requirements for "signing" a document. There are currently no regulations for establishing an "intent to sign" for electronic transactions. It is likely that legal rules will be changed on a case-by-case basis. The broad issues related to electronic commerce are being addressed in general terms. Existing laws have only been adjusted in individual cases. However, the EU Council common position on electronic signatures will have significant impact on the Swedish legal review. The proposed general law for the public sector is directed towards the recognition of digital signatures. No proposals have been advanced which would apply to Swedish society in general. Existing application-based laws (for example, customs applications) are directed towards the authentication and recognition of signatures. These application-based laws on electronic signatures are intended to protect users at both ends. No legal regulations exist with respect to the details of user equipment for electronic signatures; however, individual organisations and the SEIS Association have certain requirements. At this stage there are no particular requirements that a certification authority must meet to operate in Sweden. There are no particular liability rules that apply to the activities of certification authorities and there are no proposals to limit the liability of certification authorities in Sweden at present. The EU Council common position on electronic signatures will have an influence on this issue. No measures are currently being taken to evaluate and approve, or accredit, certification authorities in Sweden. The SEIS Association, as well as individual organisations, have made proposals for industry standards and practices for the accreditation of certification authorities. There are currently no requirements on the equipment used by a certification authority. There is ongoing work in Swedish Ministries, individual organisations and the SEIS Association for the development of certificate policies and certification practice statements. There is

ongoing work in Swedish Ministries, individual organisations and within the SEIS Association to harmonise accreditation processes and standards, certificate policies and certification practice statements.

There are currently no specific rules in Sweden allowing certification authorities to limit their liability for damages arising from a contrary use of a certificate that includes limits on its uses. There are currently no specific rules regarding the use of times of expiration in key certificates. There are currently no specific rules regarding a request to bar a key certificate by its holder. There is ongoing work in Swedish Ministries considering how global, seamless authentication and certification mechanisms should be developed. There is no general consensus in Sweden regarding the main obstacles to the growth of authentication and certification services. It is recognised that the market is not developed and that general trust is not established at this stage. Swedish law recognises electronic transactions both originating within Sweden and originating in a foreign jurisdiction. The cross-border recognition of certification has been discussed in the Cabinet Office Reference Group for digital signatures and is also being discussed in the EU Council working group on electronic signatures.

Public Sector Approaches and Private Sector Initiatives

Many public and private sector initiatives are underway in Sweden in the area of electronic authentication and certification. The ongoing work in various Ministries is considered the most important effort underway to consider these issues as it will provide the basic solutions for Swedish society. Other initiatives are also important but are company- or sector-specific. The following two reports related to authentication and certification issues have been prepared by the Swedish Government:

- *Cryptography Policy: Possible Courses of Action for Sweden*, A report from the Swedish Cabinet Office Reference Group for Cryptographic Issues, *REGERINGSKANSLIET*, Ministry for Foreign Affairs, October 1997.

- *Digital Signatures, a technological and legal overview*, Consultation Paper, Interministerial working group on digital signatures, Ministry of Transport and Communications, Sweden, February 1998.

International Aspects

At an international level, Sweden considers that the EU and UNCITRAL are presently the most important fora for discussion and resolution of the different issues related to electronic authentication and certification. Other fora might need to be involved in the future.

General

An effective legal framework that does not unnecessarily impede opportunities to conduct electronic commerce is required. As electronic commerce is global, it is important that the national legal framework is in harmony with the corresponding international system or rules. A number of initiatives have therefore been taken in Sweden to amend, where appropriate, current laws or policies that may impede the use of information technologies. In Sweden there is no specific legislation concerning digital signatures or electronic signatures and published criteria are not recognised at the national or sub-national level, thus rendering electronic documents or signatures inadmissible for evidentiary purposes. Real applications of

digital certificates currently include use by some banks, the Swedish Post, and internal applications in large governmental and private bodies. The Swedish Post offers an electronic ID-card (eID) that is a combined smart card and physical photo ID card. Sweden Post handles order, card production, and certificate production, directory with issued certificates and revocation lists and delivery. In order to obtain an eID card the applicant must appear in person at a post office. The policy and certificates are based on Swedish standards put forward by SEIS, a society with members from industry and government. The Swedish Post has recently received a contract with the government to provide eID cards and other services for the public sector. The idea is to hand out eID cards to employees. As early as 1991, the Swedish Custom Authority began to offer companies the possibility of digitally signing transactions for import and export declaration. The Central Study Support Committee (CSN) has given students the opportunity of digitally signing the obligatory declaration for student support. There are many initiatives and studies in the area of authentication in Sweden. In terms of the various options for public policy and technology architecture models for certification authorities, Sweden has developed various pilot projects. Almost all Swedish banks offer bank-services on the Internet and then use authentication methods. The Nordbank for instance, offers three basic functions, identification, authentication and encryption in a card that can be used for applications for loans, new account and access to capital savings.

Two reports related to authentication and certification issues have been prepared by the Swedish Government:

- *Cryptographic Policy*: *Possible Courses of Action for Sweden.* A report from the Swedish Cabinet Office Reference Group for Cryptographic issues, Ministry for Foreign Affairs, October 1997.

- *Digital Signatures, a technological and legal overview.* Consultation Paper, Ministry of Transport and Communications, February 1998.

Private contractual agreements

The vast majority of contractual agreements do not require any mandatory legal requirement - an oral agreement has the same legal effect as a written agreement. However, in some legal rules, requirements are laid down on legal documents being produced in a certain form in order to be legally effective. The most common requirements of form are, written format, personal signature and existence of a document as a physical original. With the exception of the form requirement mentioned above, there are no standards or procedures set forth in national law or regulation in this respect. This means that parties are free to agree on standards or procedures that suits their contractual situation. The administration of justice in Sweden is based on the principle of the free assessment of evidence. No limits are placed on sources of knowledge that may be used - the presentation of evidence is free. This principle will also apply to evidence of validity authentication methods.

Technology requirements

In Sweden, no specific legislation exists concerning digital signatures or electronic signatures.

Standards

The Secured Electronic Information in Society Association (SEIS)[31] is active in compelling and presenting requirements from industry and individual users. SEIS is a (private-sector) non-profit-making association with a membership of about 50 of the major firms and organisations in the financial, industrial, and public administrative sectors in Sweden. SEIS has developed three technical standards for electronic ID-cards, which became official Swedish standards in September 1998. These standards are:

- *Electronic ID application* - this standard describes the directory structure and data file contents for an electronic ID application implemented on a smart card.

- *Electronic ID certificates* - describes the contents of the electronic ID certificate. This standard is thus an implementation profile for X.509 certificates.

- *Electronic ID card* - this standard specifies a Swedish profile for an electronic ID card. The profile defines a number of parameters that can be regarded as part of a national PKI policy.

No law or regulation exists to govern or set standards for digital signature, electronic signatures, or other kinds of electronic authentication in Sweden. For private sector mechanisms, see the above section on SEIS. Compliance with standards is not mandatory and therefore it is unlikely that non-compliance would give rise to liability in civil proceedings. As Swedish law permits private-sector bodies to certify compliance with legislatively- or administratively-approved standards, this possibility is often used in different fields in Swedish legislation. The system with accreditation and certification can also be used when it comes to different authentication methods, such as certifying CA services.

Certification authorities

Sweden has identified the needs of the various parties who both provide and use certification services in the electronic environment. Ongoing work is carried out in finding a structure for the handling of signature keys and certificates. However, the EU Council common position on electronic signatures will have an impact on this work. No measures are currently taken to evaluate and approve or accredit certification authorities in Sweden. SEIS, as well as individual organisations, is working with standards and practices for the accreditation of certification authorities. For the moment there are no requirements on the equipment used by a certification authority. Normal Swedish tort-law will be applicable to certification authorities that have caused damages to any person who has relied on a certificate. The EU directive on a common framework for electronic signatures will contain a liability rule that will be incorporated in Swedish legislation.

Global authentication

There is no specific regulation that recognises electronic authentication used in other countries, but Swedish law recognises electronic transactions both originating within Sweden and originating in a foreign jurisdiction. The EU directive on electronic signatures contains several rules concerning qualified

[31] See http://www.seis.se

certificates issued by countries which are outside the European Community. These rules will be incorporated in Swedish legislation.

National Contact Point

- Ministry of Transport and Communications
  SE-103 33 STOCKHOLM

Switzerland

Switzerland recognises the importance of electronic authentication and certification in the context of electronic commerce. The Swiss Government is actively engaged in an examination of the legal, policy and technical standards issues related to authentication and certification technologies and mechanisms in a global networked society. Switzerland participates in a number of international activities in this area, including OECD policy discussions, UNCITRAL work to clarify legal issues, and consensus-based technical standards development. The Swiss Government supports the ongoing work of the OECD to facilitate information exchange among Member countries and the private sector, and efforts to clarify policy questions related to electronic authentication and certification.

Approaches to authentication

As part of the strategy it adopted on 18 February 1998 to promote an information society in Switzerland, the Federal Council took the immediate step of instructing the federal administration to introduce electronic signatures, design a public key infrastructure for their use and work out the necessary regulations. To that end a questionnaire was presented to the interested parties for the purpose of determining how the work should be conducted. Once the replies had been studied, an *ad hoc* working group developed a public key infrastructure model, which was presented at a public conference on 24 November 1998 together with a notice from the Federal Office of Justice on the legal value of the electronic signature. By and large, participants from the public and private sectors supported the work underway. The setting up of a public key infrastructure was regarded as a matter of urgency and it was felt that the question of the legal value of the electronic signature should be examined in parallel as soon as possible and should if necessary be resolved in stages.

Legal value

Whether an electronic signature has legal value and is equivalent to a written signature is seen as crucial. According to the aforementioned notice from the Federal Office of Justice, it would not be possible to deny the electronic signature any legal value under existing Swiss law, even if its equivalence to the written signature is not enshrined therein. Since most deals made via electronic media do not require a written signature as defined in articles 12 ff. of the Code of Obligations, there is nothing to prevent the use of new communications technologies for signing contracts or placing orders. Emphasis should rather be placed on the secure identification of the parties and on the integrity of the data messages exchanged. From this point of view, provision of a secure public key infrastructure, recognised by the Confederation, should help to promote electronic commerce in Switzerland. The advantage of such a measure is that it can be achieved quickly through an ordinance issued by the Federal Council, pending more complete legislation addressing those aspects of private law that are related to the legal equivalence of the electronic

signature and the written signature. The experiments carried out in the initial phase will enable the authorities to draw up general regulations with the benefit of a sound knowledge of the issues.

Public key infrastructure model

The general model for the planned public key infrastructure is derived to a large extent from the Swiss accreditation system (http://www.sas.admin.ch). Certification authorities who wish to be officially recognised must first obtain confirmation, from a "certification body" approved by the Swiss Accreditation Service, of their compliance with the essential requirements for guaranteeing the security and reliability of the electronic signature.

Ordinance on electronic signatures

The draft ordinance[32] on electronic signatures therefore deals only with the setting up of a public key infrastructure. The draft first sets out the essential requirements to be met by certification authorities who wish to be recognised. As stated above, assessment of conformity with essential requirements is left to the private sector, i.e. to accredited certification bodies. The draft ordinance regulates the obligations which will be binding on recognised certification authorities. For the purposes of ensuring that the author of a data message can be identified from an electronic signature, the certification authority has to check the identity of persons applying for electronic certification in appropriate ways; in particular by requiring them to be present in person at the time of registration and provide valid proof of their identity. The range of services to be offered by recognised authorities must also be determined; these may include providing access to directories of electronic certificates. They are responsible for the revocation of electronic certificates and are required to keep certificate revocation lists. The ordinance includes further provisions on the keeping of electronic certificates, not only while they are valid but also after they have expired and in cases where those who issued them have ceased to operate. Supervision of recognised certification authorities is the responsibility of the body that officially recognised them. If the former cease to fulfil the essential requirements or fail to respect their obligations, it must be possible to revoke recognition. The question of the responsibility of recognised certification authorities, either to their customers or to third parties who place their confidence in the certificates they issue, is one that warrants very special attention. It is not certain, however, that the matter can be dealt with exhaustively merely by a Federal Council ordinance. The essential requirements, which aim to ensure that the recognised certification authorities have a sound capital base, should in any event guarantee their ability to cope with compensation demands. In order to guarantee that they can be used in conjunction with systems in place abroad, the draft ordinance provides for mechanisms that encourage recognition of foreign certification authorities. Finally, it is up to the Federal Council to delegate the task of drafting provisions on important points of detail, especially where the essential requirements are concerned. The draft ordinance is available at the internet site of the Federal Office for Communications (http://www.bakom.ch). The ordinance and its implementing provisions should enter into force at the beginning of the year 2000.

[32] The draft ordinance is a proposal by the aforementioned *ad hoc* working group.

Certification authorities

Swisskey is the first and the only Swiss certification authority (http://www.swisskey.ch). The major Swiss banks will soon be using this company's services to modernise their telebanking facility. The Federal tax authorities have recognised the certificates issued by Swisskey in pilot projects.

National contact point

It is possible to obtain further information at digsig@bakom.admin.ch

Turkey

Authentication

Turkey uses digital signature software for RSA and DSA, and is trying to implement some elliptical curve digital signature algorithms as well, but none of these algorithms are in common use in Turkey. Some banks use secret key cryptography to establish identity in their closed networks. There is no legislation for electronic authentication in Turkey yet. However, public and private sectors are aware of such a need for identity establishment in order to communicate securely over public networks. A report submitted by the Electronic Commerce Co-ordination Committee (ECCC) to the Turkish Government in May 1998 suggests that legislation for clear description of the liabilities of entities which offer cryptographic services, keep or distribute cryptographic keys, should precede legal acceptance of electronic signatures.

Certification

For the entities that both provide and use certification services in the electronic environment, Turkey believes that the first requirement is the establishment of a trust mechanism for cases related to self-certification, rather than the needs of the entity. Here the Turkish government uses the word "certification" as restricted to the "certification of public key / personal identity pairs" to avoid confusion in terminology issues. Where "digital certificate" is used in relation with public key cryptography, as the "digital certificate, which is digitally signed by the certification authority, of the data message originator to confirm his public key / personal identity pair", in Turkey there is no "digital certificate" used in commerce. This is because, as is the case with many other countries, Turkey has not yet established a public key infrastructure. It is not generally decided whether public key cryptography or any other mechanism will be used for establishing information security over public networks. However, the Turkish Electronic Commerce Co-ordination Committee (ECCC), has held meetings since February 1998 with members from 37 public and private sectors to develop business practice guidelines for certificate-issuing entities required for the public key infrastructure. It is Turkey's view that once the public key infrastructure (or a similar functioning mechanism) is globally established -- a global network is formed with each user having a unique digital certificate which indicates a trusted personal identity and/or public signature key pair -- then there will be no need for separate certification of a broad class of information, since the source of information can be identified by verifying a reliable digital signature. Once "certification of personal identity and/or public key pairs by certification authorities" can be achieved globally by generally accepted public key cryptographic algorithms (or some similarly functioning and globally compatible method or group of methods can be put into operation over public networks), certification of various kinds of information online will follow automatically.

The technical group of Turkish ECCC is considering suggesting a single certificate, namely, a unique identity certificate which would belong to a person or an entity, if it is generally agreed that a public key infrastructure should be established. Turkey believes that related laws should be flexible enough to take account of further technological developments. Restricting the discussion on certification to the "certification of public key and/or personal identity pairs" as mentioned above, Turkey believes that the main problem in public key cryptography is to establish the certification mechanism, which will be local enough to assure correct determination of personal identities, and yet, global enough to use worldwide standard key generation algorithms. Hence, Turkey is also examining architecture models other than public key infrastructures, which will be directed towards both the public and private sectors. The Turkish government believes that it is premature to discuss architectural models in Turkey, as in many other countries. However, Turkey is preparing for pilot projects and seeking ways to establish user awareness about different aspects of communication over public networks.

Authentication, Certification and Related Services

All administrative, governmental, private commercial and consumer transactions are areas for the potential application of authentication and certification services. There are no such requirements in Turkey for establishing of document integrity; however, the Turkish ECCC may suggest requirements such as digital signatures and time stamps.

Legal and Policy Issues

In the Turkish legal system there are two laws which impose "quill and pen" requirements regarding written documents: The Act of Contracts and the Civil Procedural Act. The Act of Contracts requires a "signature" as a validity condition for all written contracts;[33] it also stipulates the signature as a handwritten one.[34] In accordance with the Civil Procedural Act, legal transactions with values above TRL 20 million must be proved by "decisive evidence".[35] A "written document" is an important piece of decisive evidence identified in the Civil Procedural Act. However, such a document must be signed with a handwritten signature as described above.[36] For electronic transactions that are carried out in a closed network, "intent to sign" is established when the participants of the network sign the contract regarding the operation rules of the network. This kind of transaction is normally carried out among the banks. Turkey believes it is premature to be completely specific on the national provisions and laws that require amendment in accordance with UNCITRAL Model Law, since the Model Law itself is in the formation stage. Nevertheless, by taking into consideration all 17 articles of the Model Law, one may stipulate that the Turkish Act of Contracts, Civil Procedural Act, and some provisions of the Commercial Code are among the laws to be amended. Currently two initiatives have been carried out in Turkey related to authentication and certification. First, a recently created sub-committee of the Electronic Commerce Co-ordination Committee has prepared a report on legal issues which takes into consideration all the international documents on the issue, and highlights the important points to be modified. The Model Law is one of the documents emphasised by the Sub-Committee on Law. Second, the Ministry of Justice has

33 Article 13.

34. Article 14.

35. Article 28.

36. Articles 13 and 14.

set up a new working group to amend the Law of Contracts. Since the work of the group is at the preliminary stage, it is too early to make any reference to a specific provision on the issue.

In the existing legal system, general issues related to electronic commerce are addressed within the provision of written contracts. As the work of the Electronic Commerce Co-ordination Committee is not yet complete, it has not been decided whether specific new laws will be proposed or existing laws will be amended. It is not even clear if certification authorities will be established like public notaries, where appointment and supervision are carried out by the Ministry of Justice, and which are fully liable for the certification of the signature belonging to a specified person. There is no specific law currently proposed for authentication and certification in Turkey. However, the Ministry of Justice has prepared a draft act on the protection of personal data based on the basic principles from the Council of Europe Convention. The EU Directive 95/46 and individual legislation of European countries have also been examined during preparations. Turkey believes that the main obstacle to the growth of authentication and certification services based on public key cryptography is the difficulty in establishing the certification mechanism, which will be local enough to assure correct determination of personal identities, and yet, global enough to use worldwide standard key generation algorithms. Hence, as mentioned above, Turkey is studying compatible architecture models other than public key infrastructures as well, which will be directed towards both the public and private sectors. Currently, the national laws of Turkey do not recognise any kind of electronic transaction regardless of its origin. Cross-border recognition of certification may also be regarded as the subject of a public key cryptographic application, upon which global agreement has not yet been reached. Once the certification of personal identity and/or public key pairs by certification authorities can be achieved globally by generally trusted public key cryptographic algorithms, or other compatible architecture models can be put into operation over public networks, Turkey will be in a position to take the necessary steps for cross-border recognition.

Public Sector Approaches and Private Sector Initiatives

Although not related to authentication and certification directly, organised public sector developments on electronic commerce in Turkey, which have an indirect influence on authentication and certification, began in 1995. The Turkish Export Promotion Centre (EPC) and Information Technologies & Electronic Research Institute under the Scientific & Technological Research Council of Turkey (Tübítak-Bílten) proposed a pilot project for electronic commerce, and UNCTAD declared the Export Promotion Centre (EPC) as "Ankara Trade Point" in April 1997. In an August 1997 meeting under the authority of the Prime Minister, the High Council for Science and Technology emphasised the establishment of i) a national information infrastructure, and ii) a network for e-commerce. The Council also decided to set up an Electronic Commerce Co-ordination Committee (ECCC). The Turkish ECCC, which includes members from 37 public and private sectors, held its first meeting in February 1998 and submitted its first report in May 1998. Under the auspices of the Information Technologies & Electronic Research Institute under the Scientific & Technological Research Council of Turkey a project to prepare the "Masterplan for the Turkish Information Infrastructure (TUENA)" began in July 1997.[37] Another project called "Public-Net (KAMU-NET)" for an active public service network was organised under the co-ordination of the Prime Ministry.

[37] For a detailed summary of the *TUENA* project, see http://www.tuena.tubitak.gov.tr

International Aspects

Meetings organised by OECD and other international organisations, as well as the communication over public networks themselves, form the most appropriate fora for discussion and resolution of issues related to authentication and certification over public networks.

General

There are some activities like the pilot projects held by the Turkish Electronic Co-ordination Committee (ECCC), the Undersecretariat of Foreign Trade and the Undersecretariat of Treasury, as well as the modernisation and computerisation projects of Turkish Customs (described below) and banks, all of which use some kind of authentication mechanisms, not necessarily in the narrow sense of public key cryptography. Many Turkish banks use electronic authentication mechanisms for the security of electronic communication between the customer and the bank's ATM (Automatic Teller Machine). Some of these banks also have Websites on the Internet, and conduct pilot projects that employ public key cryptography for privacy, but not for authentication purposes, since the latter requires digital certification of all bank customers.

Private Contractual Agreements

In Turkish legislation electronic signatures (including digital signatures and others) have not yet been regulated. In principle, as has been emphasised in the Act of Contracts (Article 11), there is no validity requirements as to the format of the private contractual agreements unless the contrary is stipulated in the Acts. In the framework of this principle, contracts concluded by electronic signatures are perfectly valid for private parties. Nevertheless, the question of the evidence of proof under the Civil Procedural Act arises for this type of validly concluded form-free contracts. Whenever there is a form requirement stipulated in the Acts, electronic signature shall not be recognised as a valid signature (which is legally expected to be a handwritten one under Article 13 of the Civil Procedural Act), and this will negatively affect the contract validity. Under the Act of Contracts, parties are free to agree to standards, procedures and uses which are not considered in law specifically obligatory for contracts. Nevertheless, whenever they agree on a certain procedure in accordance with form-free contracts, they are obliged to follow this procedure as underlined in Article 16, par.2 of the Act of Contracts. As long as the chosen procedure is not the decisive one described in the Acts, the parties may attain redress under the terms of the contract. As to the evidentiary standards concerning the methods of proof, the Civil Procedural Act stipulates in Article 288 that, transactions valued TRL 20 million or above shall be proved by decisive evidence. Among the decisive evidence listed in numerous clauses in the Act, a written document has also been underlined as evidence. Since Articles 13 and 14 of the Act of Contracts describes the written document as signed with a handwritten signature, contracts signed with electronic signatures will face difficulties during judicial or administrative proceedings concerning the issue of proof.

Standards

There is no standard developed for the specific branch of digital signatures. Turkish banks that employ electronic authentication for communication between customers and ATM comply with some international standards. The private sector is willing and motivated to play a role in developing and certifying standards for digital signatures etc.

Certification authorities

The concept of a "certification authority" is introduced as a part of public key infrastructure and public key cryptographic applications, upon which global agreement has not yet been reached. Turkey closely follows the progress of discussions, and waits for universal agreement before taking such detailed measures and precautions.

Global authentication

Turkey does not yet recognise digital signatures or other kinds of electronic authentication used in other countries, nor is there a law or regulation on electronic authentication. As mentioned above, the concept of "cross-certification" is also introduced as part of public key infrastructure and public key cryptographic applications, upon which global agreement has not yet been reached. Turkey closely follows the progress of discussions, and waits for universal agreement before taking such detailed measures and precautions.

Additional Information from the Turkish Customs Undersecretariat

Turkish Customs has embarked upon a major modernisation and computerisation reform that is partly funded by the World Bank. The pilot phase is now complete, with a new computerised clearance system implemented at one of the busiest Customs offices in Turkey — Istanbul international airport. At present, Customs partners (brokers, importers, exporters, and transporters) must utilise a kiosk facility at the Customs office to input details to the new system to facilitate the clearance of their consignments. Data entry is controlled by a combination of user code, password and tax identification number protection. System users are registered after verification of their credentials from their applicable trade association. An EDI capability is currently being developed for implementation in mid-1999 that will avoid redundant data entry. Using EDIFACT standards, Customs partners will eventually be able to submit electronic manifest and declaration data directly from their own systems to any of 50 computerised Customs offices. CUSCAR and CUSDEC messages sent by Customs partners through an EDI gateway will be similarly subject to identification, password and tax identification controls, with a further layer of security provided by the X.435 protocol. Smaller customs partners that do not possess a sophisticated computer system will also be accommodated, as they will be able to access a secure Website based on Secure Socket Layer (SSL) technology. Manifest and declaration data can be input via the Internet by this method with the same identification and password controls. The data processed by the secure Website will be transformed into EDIFACT format and channelled with other EDI traffic from larger and more traditional Customs partners. Customs partners who wish to use the EDI interface to Customs, either directly or via the Internet, must first register and receive a user code and password specific for this purpose.

Customs Law and regulations were followed in Customs offices where customs procedures were implemented manually. Customs procedures carried out in the computerised customs offices are not clear and conflict with the existing legislation in some respects. For this reason, a new regulation was issued for the computerised customs offices and in this way the computerised customs procedures were legalised. In this regard, one of the most significant developments is that the declarant can input the declaration details to the customs computer system by means of a kiosk facility in the computerised customs offices (when an EDI project is introduced he/she can generate the details in EDIFACT standard in his/her office and

send electronically to the customs computer system) while the customs official receives, approves and then registers the declaration in those customs offices where the customs procedures are implemented manually. Another development is that the difference between the commencing date of liability for payment of customs tax and duties and commencing date of liability for payment of VAT at the importation is removed to preclude duplication of customs tax and duty calculations, with an amendment to the 1998 VAT Law. Thus, the calculations can be realised accurately in the computer environment.

National Contact Points

- Meral Özaygen
  Tel: + 90 312 324 24 07

- Turkish Ministry of Justice
  Ayse Saadet Aríkan
  Tel: + 90 312 231 49 19
  E-mail: da04-k@tr-net.net.tr.

- Turkish Electronic Co-ordination Committee (ECCC) and Turkish Undersecretariat of Foreign Trade
  Varol Atabay
  Tel: + 90 312 215 06 80

- Turkish Undersecretariat of Treasury
  Inci Apaydin
  E-mail: apaydini@pm.treasury.gov.tr

- Turkish Undersecretariat of Customs
  Nurcan Özyazici
  E-mail: nurcan@gumruk.gov.tr

- Scientific and Technical Research Council of Turkey
  Melek D. Yücel
  Tel: + 90 312 210 12 61
  E-mail: yucel@ea.eee.metu.edu.tr.

- Turkish Banks
  Ilker Kuruöz
  E-mail: ilkerk@garanti.com.tr

United Kingdom

Authentication

There are currently no prescribed methods for establishing identity in the electronic environment in the United Kingdom. In practice, Certification Authorities (CAs) typically use passports, driving licences, birth certificates and utility bills to confirm the identity of their clients. The United Kingdom is planning to introduce legislation in late 1999 (as noted in the Secure Electronic Statement by the Department of Trade and Industry (DTI)) aimed at helping electronic commerce flourish through the use of electronic authentication. This legislation is designed to allow for the voluntary approval of certification authorities and the legal recognition of electronic signatures. In terms of paving the way for new technical standards to help spread the inexpensive use of this technology, the DTI is actively supporting the development of standards (in the EU and ISO/CEN/CENELEC/ETSI) as well as promoting the use of smart cards which is seen as salient for the widespread use of electronic signatures in the public.

Certification

The United Kingdom has identified the needs of the various parties who both provide and use certification services in the electronic environment and as a result it intends to introduce licensing arrangements allowing certification authorities to demonstrate that they meet the standards which users will expect. Digital signatures certificates are already in use in the banking and financial services sectors, although mainly between users in "closed" groups. Some initial offerings of certificates are being made in the open environment by the UK Post Office. The United Kingdom is considering how business practice guidelines for entities issuing "digital" certificates can be developed. It sees the main guidelines applying to the providers of services as opposed to the users. The ongoing evolution of commercial practices and technical standards development -- which are extending the use of existing technologies and practices toward new applications for "certifying" various kinds of information on-line -- is reflected in public policy discussions in the United Kingdom. In particular, the government intends to make extensive use of electronic signature technologies in the delivery of services to the citizen and in public procurement. The United Kingdom intends, subject to legal considerations in national law and in the EU, to recognise both identity and authorisation, and entity, certificates. United Kingdom legislation will be sufficiently flexible to cater for new technological developments. The development of a public key infrastructure for both the private and public sectors based on "horizontal" architectures will be promoted. The United Kingdom does not envisage the development of a single root CA. There are no current, or planned, restrictions on the use of authentication or certification mechanisms in the United Kingdom.

Authentication, Certification and Related Services

The areas of potential application for authentication and certification services (administrative, governmental, private commercial transactions, consumer transactions) in the United Kingdom are seen as limitless. It is perceived that electronic signature services will be used wherever secure electronic commerce or other security requirements (involving integrity) are relevant. There are presently no legal requirements for ensuring the integrity of data for electronic transactions and commerce, although business would typically cover such requirements in contracts.

Legal and Policy Issues under Consideration

There are many provisions in British law which impose requirements that only written (or physical) signatures can satisfy legal requirements for "signing" a document. Examples include legislation relating to Wills, deaths, marriages and the sale of land. There is no established practice at present on how the "intent to sign" is established for electronic transactions in the United Kingdom. No specific provisions of national laws or rules would have to be modified to accommodate the provisions of the UNCITRAL Model Law on Electronic Commerce, in that the Model Law is not mandatory. The United Kingdom is, however, attempting to adopt the relevant portions of the Model Law within proposed legislation on electronic signatures. In terms of addressing the general issues related to electronic commerce, the United Kingdom does not see any need to amend the general legislation relating to commercial trade. As already mentioned, specific legislation on electronic signatures is being prepared. The proposed legislation is directed towards electronic (not just digital) signatures, certification authorities and also those bodies (which are referred to as Trusted Third Parties) offering encryption services. As the legislation is developed, user interests (in relation to privacy and consumer protection) will be fully taken into account. There are no requirements in the United Kingdom on user equipment, the electronic signature itself, the use of chip cards, key lengths etc., used in authentication technologies.

There are currently no regulations specifying the requirements that a certification authority must meet to operate in the United Kingdom. There are currently no particular liability rules applying to the activities of certification authorities in the United Kingdom. In the proposed legislation, it is intended that the liability of certification authorities (in relation to negligence) to their clients and also third parties relying on their actions, will be limited. The proposed legislation will include criteria to evaluate and approve, or accredit, certification authorities. The United Kingdom is considering BS 7799 as a base requirement for accrediting CAs as well as the ITSEC Scheme (in relation to the assurance of the CA's IT). There are no requirements at present on the equipment used by a certification authority in order for a certification authority to be accredited. In terms of the development of certificate policies and certification practice statements, work is on-going in relation to the development of the legislation and the discussions on the EU Directive on electronic signatures. Measures have been proposed to harmonise accreditation processes and standards, certificate policies and certification practice statements in relation to the discussions that are taking place on the EU Directive on electronic signatures. Although there are no specific rules at present, certification authorities in the United Kingdom are entitled to limit their liability for damages arising from a contrary use of a certificate which includes limits on its uses. A key certificate used may contain a time of expiration but there are no specific rules at present. The holder of a key certificate in the UK requests the certification authority to bar the key certificate, and the "barring" would have to take immediate effect. Such requirements will be covered in the proposed legislation. The United Kingdom is considering how global, seamless authentication and certification mechanisms should be developed through its support of the work of UNCITRAL on Uniform Rules for electronic signatures and its desire for the OECD to also produce guidance materials for CAs. A lack of trust and confidence on behalf of the user and also a lack of awareness in many market sectors are regarded as the main obstacles to the growth of authentication and certification services in the United Kingdom. Although the law does not recognise electronic transactions in any uniform sense at present, there is no discrimination based on whether the transaction originates from within the United Kingdom or from a foreign jurisdiction. The proposed legislation will deal with the cross-border recognition of certification in parallel with EU Directive provisions.

Public Sector Approaches and Private Sector Initiatives

There are many different initiatives in the private sector, in addition to the government's development of legislation, in the area of electronic authentication and certification. The most important efforts currently underway are seen as those at the international level.

International Aspects

The EU and UNCITRAL are the most important fora for discussion and resolution of the different issues related to electronic authentication and certification at present. However, the United Kingdom also wants the OECD to be involved in policy guidelines for the way certification authorities function.

General

Following upon the October 1998 *Ministerial Declaration on Authentication for Electronic Commerce*, the inclusion of measures in the proposed Electronic Commerce Bill will give legal recognition to electronic signatures and electronic writing and allow the progressive use of electronic signatures in the citizen's dealings with Government. This is in keeping with the UNCITRAL Model Law. Common law and Contract law apply at present to matters concerning digital signatures, electronic signatures, or other kinds of electronic authentication, but the proposed Legislation will ensure legal recognition of electronic signatures and electronic writing, make provision for a voluntary approvals regime for Trusted Service Providers and implement the EU Electronic Signatures Directive. Organisations offering certificates include BT (offering Verisign certificates) and the Post Office (offering ENTRUST certificates). At present, trials - for example, Barclays Endorse Service being used in a Department of Social Security project - are taking place. The Government's target is that 25% of government service forms will be available by 2002, and 100% by 2008. A government PKI based solution is being developed, with private sector involvement (Baltimore and Racal) under the Cloud Cover banner. In the private sector, the UK Alliance for Electronic Business (AEB) is setting up an industry led scheme, in co-operation with partners in other countries, for accrediting Certification Authorities, setting standards, international co-operation etc. (The project is called "Emeritus").

Private contractual agreements

Private parties are free to decide on their own protocols etc. for using electronic messaging. In the event of a contractual dispute normal Contract Law would apply. There are no mandatory standards or procedures in existing or proposed legislation. The proposed legislation will establish a voluntary licensing regime. Since there will not be any mandatory standards in the United Kingdom, parties will not need to use the national legal system to attempt to attain redress under the terms of the contract. The policy concerning evidentiary standards is not yet finalised - the proposed legislation will deal with the legal recognition of electronic signatures.

Technology requirements

There is no legal framework for approval of electronic authentication methods at present and, in any case, it will be voluntary. To date, British law does not identify certain electronic authentication technology as secure, but it will do when the European Electronic-signatures Directive is implemented into UK law, in

that technologies which meet the objectives set out in the Directive will carry a certain advantage in the marketplace. Advanced Electronic Signatures will be those that meet the higher requirements set out in the Annexes of the Electronic Signatures Directive.

Standards

No national or sub-national standards for electronic authentication have been developed by the public or private sectors yet in the United Kingdom, but work is taking place in the context of CEN/ISSS and ETSI. There are no UK laws governing the development of standards. National Standards are developed by BSI working under Royal Charter. Under the proposed legislation the voluntary licensing regime for Trust Service Providers will require that applicants meet performance objectives. Any relevant national or international standards will be taken into account in establishing these objectives. The private sector supports activities in international standards fora such as ISO, IEC, CEN/CENELEC, ETSI etc, and private-sector bodies can be accredited to carry out third party evaluation against agreed standards. The Alliance for Electronic Business (AEB) is promoting a "Global Trust Service Infrastructure" in association with partners in other countries.

Certification authorities

A voluntary licensing regime will be set up under proposed legislation to evaluate and approve, or accredit, certification authorities. British law does not yet govern or set requirements for licensing or accrediting "certification authorities", but the general approach will be covered under the proposed Legislation and the details set out in secondary legislation. The requirements in the proposed EU Electronic Signatures Directive will apply to the liability rules applied to the activities of certification authorities. The nature of the liability regime under the proposed UK legislation is under consultation.

Global authentication

There is no law at present that distinguishes between domestic and foreign trust services. The recognition that exists does so by default, since under UK law there is no prohibition on their use. In addition, no limitations are placed on cross-border recognition of electronic authentication. Mutual recognition can be achieved now by private arrangement and the proposed legislation will have to deal with the issue of how foreign TSPs are to be accommodated. In the broader context, the UK Government will work with other countries to promote the wider recognition of authentication services, cross certification and mutual recognition. The proposed legislation will provide for a statutory voluntary approvals regime, but the government has announced that it will only use the powers if industry fails to put in place a suitable non-statutory self regulation scheme. In the private sector, The Alliance for Electronic Business is proposing to offer such services, but will not have a monopoly. It is not envisaged that there will be regional variations in cross-certification procedures.

National Contact Point

- Information Security Policy Group
  Department of Trade and Industry
  Tel: + 44 207 215 1962
  Fax: +44 207 931 7194

- John Smith
  Tel: +44 207 215 1961
  E-mail: john.smith@dti.gov.uk

- Geoff Smith
  Tel: +44 207 215 2940
  E-mail: geoff.smith@dti.gov.uk

United States

General

In the *Framework for Global Electronic Commerce*, released in July 1997, President Clinton directed among the critical issues related to a uniform commercial code, that "[t]o encourage electronic commerce, the U.S. government should support the development of both a domestic and global uniform commercial legal framework that recognises, facilitates, and enforces electronic transactions worldwide." The focus, in developing policies and practices, is on the predictability of the transaction, of which the issues related to authentication are one subset. In stating the principles that guide U.S. policy, President Clinton noted:

> "In general, parties should be able to do business with each other on the Internet under whatever terms and conditions they agree upon. Private enterprise and free markets have typically flourished, however, where there are predictable and widely accepted legal environments supporting commercial transactions. … Fully informed buyers and sellers could voluntarily agree to form a contract subject to this uniform legal framework, just as parties currently choose the body of law that will be used to interpret their contract. Participants in the marketplace should define and articulate most of the rules that will govern electronic commerce. To enable private entities to perform this task and to fullfil their roles adequately, governments should encourage the development of simple and predictable domestic and international rules and norms that will serve as the legal foundation for commercial activities in cyberspace."

In carrying out this objective, the United States government (USG) has utilised the relevant provisions of the UNCITRAL Model in the development of policies and in reviewing legislation proposals. The relevant provisions of the Model Law have also been the basis for substantial action at our sub-national or state level, including efforts by the state law experts to prepare a Uniform Electronic Transactions Act (UETA). The relevant provisions of the Model Law have also been a foundation for the USG proposal for an International Convention on Electronic Transactions. At the international level, to enable global electronic commerce, the United States supports both a domestic and global uniform legal framework that recognises, facilitates, and enforces electronic transactions worldwide. The principles and objectives outlined above have been incorporated into a proposal for a multilateral Convention on Electronic Transactions. The Convention proposal recognises that The United Nations Commission on International Trade Law (UNCITRAL) has completed work on a Model Law on Electronic Commerce that supports the

commercial use of international contracts in electronic commerce. The Model Law establishes rules and norms that define the characteristics of a valid electronic writing and an original document, provides for the acceptability of electronic signatures for legal and commercial purposes, and supports the admission of computer evidence. It also validates and recognises contracts formed through electronic means, setting default rules for contract formation and the governance of electronic contract performance.

While many countries, including the United States, are using the Model Law as a basis for updating their commercial laws, many countries are not. The United States Government supports the adoption of the enabling principles that are contained in the Model Law through a binding international agreement as a start to defining an international set of uniform commercial principles for electronic commerce. On the international level, a number of countries are considering or have enacted digital signature legislation to specifically address authentication methods including digital signatures. Recently, UNCITRAL began work in the authentication area, specifically including digital signatures, and is currently considering model statutory provisions. Since UNCITRAL began its work in 1997, new models for the implementation and use of digital signature technology are emerging. The expanding array of authentication methods and the complexity of their commercial use raise concerns about fashioning detailed legal rules at this point in such areas as, for example, certificate authorities and liability. As noted above in the discussion of domestic legislative developments in the United States, most states have rejected statutory enactments setting forth specific rules for digital signatures. Instead, the trend is toward enabling and supporting legislation that supports the use of electronic signatures (digital signatures and other authentication approaches) appropriate to the circumstance, but which otherwise does not impose liability or licensing schemes. Not surprisingly, the USG proposal for a Convention has been recognised and encouraged by state government leaders working on the cutting of service delivery and legal issues related to authentication. [See "A Joint Resolution On Electronic Commerce by the Electronic Commerce Co-ordinating Council and the National Association of State Information Resource Executives, the National Association of State Purchasing Officials, and the National Association of State Comptrollers", August 1998, www.doc.gov/ecommerce/eccc.htm].

This new legislative approach reflects important evolutionary market changes. In particular, the market appears unlikely to settle on one universal authentication mechanism or model of implementation in the near future. Parties appear headed toward a choice between different types of authentication regimes, depending on the nature of the transaction and upon the prior relationship, if any, among the parties to the transaction. For example, a large company may choose one authentication method for the electronic system used to procure goods from suppliers but a different method for on-line purchases by its customers. Like other aspects of electronic commerce, authentication methods and technologies are developing rapidly. In the area of digital signatures, the technology is being implemented in ways that are different from the pubic key infrastructures envisaged when the first digital signature legislation was passed. For example, digital signatures may be used for purposes such as establishing "attributes" like age, authority, etc. which may go beyond verifying identity or achieving non-repudiation. In addition, electronic transactions are, for the foreseeable future, predominantly occurring in "closed" or "bounded" rather than in so-called "open" systems predominated by "strangers"; i.e. users with no contractual or other relation or nexus. There is also recognition that digital signatures are being used for a great number of business purposes apart from those originally envisaged; for example, minimal value certificates are already being issued on a wide scale basis. The USG supports the development of structures that will support a variety of authentication methods and technologies as well as a variety of implementation models. Fashioning rules that would govern digital signature technology or any other single authentication technology, to the exclusion of other authentication approaches, would inhibit rather than

encourage the growth of electronic commerce. The USG recognises the valuable dialogue supported by UNCITRAL on these issues.

The Convention would remove paper-based obstacles to electronic transactions, and address electronic authentication issues. It would have two elements:

Part A: General Obligations
These would include: minimal modification to existing legal rules and minimal adoption of new rules; technology and implementation neutrality; a non-discriminatory approach toward authentication technologies and business applications from other countries; the avoidance of unnecessary barriers to trade. In addition:

- **Party Autonomy**
  Parties to a transaction should be permitted, to the maximum extent possible, to determine by contract the appropriate technological and business methods of authentication. There should be assurance that those means will be recognised as legally binding, whether or not those technological and business means are specifically referenced in legislation or regulation. The terms of any agreement (including closed systems) between parties governing their transaction should be enforced without regard to any statutory framework governing electronic authentication.

- **All Authentication Technologies and Business Methods May Be Evidence of Authenticity**
  Where the law requires evidence of the authenticity or integrity of a message, a party should be permitted to use any authentication technology or business method to try to prove authenticity, whether or not such authentication technology or business method is specifically referenced in legislation or regulation. (As with the authentication of physical documents, a party denying the agreement could introduce evidence disputing its authenticity or integrity and the issue would be resolved by the trier of fact).

Part B: Adoption of Key Elements of the Model Law on Electronic Commerce
Enabling provisions drawn from the provisions of the UNCITRAL Model Law on Electronic Commerce would define an international set of uniform commercial principles for electronic commerce. The Convention would recognise the acceptability of electronic signatures for legal and commercial purposes, define the characteristics of a valid electronic writing and an original document and support the admission of electronic evidence and their retention of records.

Discussion of the Convention proposal began in the Working Group of UNCITRAL, held in New York City on 29 June – 10 July 1998. Parallel efforts are also underway in bi-lateral discussions. For example, in the "French-American Background Paper on the Challenges of the Information Society and the Digital Economy", the respective governments agreed on a number of guidelines to promote electronic commerce, including the following:

> "…the Governments should support a global legal framework that recognises, facilitates, and enforces electronic transactions worldwide. The commercial legal framework should include a multilateral convention that recognises the validity of electronic signatures for commercial purposes and allows parties to determine through a legally valid contract the appropriate

> technological and business methods of authentication for their transaction." [18 June 1998] [See www.doc.gov/ecommerce/US-FRJntStmnt.htm]

The principles embodied in the USG proposal on a Convention have also been reflected in the US-Japan Joint Statement on Electronic Commerce, signed on 15 May 1998. [See www.doc.gov/ecommerce/usjapan.htm]. Similarly, in the Joint Statement between the Governments of Australia and the United States [See http://www.doc.gov/ecommerce/AUfinal.htm], it was established that both Governments:

> " …should work towards a global framework that supports, domestically and internationally, the recognition and enforcement of electronic transactions and electronic authentication methods (including electronic signatures). At an international level this should include exploring the possibility of a convention or other arrangements to achieve a common legal approach that will support electronic transactions as well as a variety of authentication technologies and implementation models."

The principles have also been incorporated into bilateral statements with the governments of Korea [see http://www.doc.gov/ecommerce/koreajs.htm] and with the United Kingdom. Ministers meeting in Ottawa for the OECD Conference issued a "Declaration on Authentication" that reflects these principles and policy objectives. In choosing to give priority attention to enabling electronic transactions, the policy underlying the *Framework for Global Electronic Commerce* recognises the pre-eminent role of the private sector in using and developing technologies and adopting standards. The *Framework for Global Electronic Commerce* also recognises the diversity of business models and implementations that are emerging on a worldwide scale -- for electronic commerce generally, as well as elements related to electronic transactions, including authentication. At the national level, no such specific law or regulation exists with regard to private sector contractual arrangements. With regard to the use of cryptographic digital signatures by agencies of the federal government, use is subject to the Information Technology Management Reform Act of 1995 (formerly the Computer Security Act).

It is important to understand that under US law, there is no pre-eminent federal "law of contract" for the broad array of commercial transactions that take place both domestically and internationally. The constitutional framework recognises that that this area is the privy of state governments. On the whole, state legislatures -- often with the advise of private sector commercial law experts -- are taking on the challenge of adapting existing rules to the electronic environment. As of the end of 1998, 44 states had adopted some form of law updating their statutes in the area of electronic transactions. The vast majority of these actions -- by 40 states -- involved taking the minimalist, enabling steps of ensuring that electronic signatures are not denied legal effect simply because they are in electronic form, consistent with the UNCITRAL Model Law on Electronic Commerce discussed below. [See "Scope of Authorisation to Use Electronic Signatures in *Enacted* Legislation" (Last Updated 5 April 1999), www.mbc.com/legis/table01.html]. Although a small handful of states have specifically identified cryptographic *digital* signatures in their laws to facilitate transactions and filings (notably, the statutes passed in Utah, Minnesota, Missouri and Washington), it appears that legislatures are preferring most minimalist, enabling approaches. As one private sector survey noted, "… it is apparent that the comprehensive prescriptive approach characterised by Utah's statutory and regulatory scheme is no longer leading the way and may be, in fact, disfavoured." [See ILPF, "UPDATE: Survey of State Electronic & Digital Signature Legislative Initiatives", www.ilpf.org/digsig/UPDATE.html].

This trend in state legislature is also reflected in the efforts by national organisations, like the National Conference of Commissioners of Uniform State Laws (NCCUSL), to develop model uniform approaches. The activities of groups like NCCUSL, among others, do in fact represent consensus among state law experts about the direction and substance of legal policy that often are the antecedents to significant statutory changes made by state law-passing bodies. In this area, NCCUSL had undertaken a project to prepare a Uniform Electronic Transactions Act (UETA). The initial focus of NCCUSL was a broad, detailed draft framework that focused on establishing the necessary conditions for acceptance of the trustworthiness of electronic signatures. Over the last two years of its work, NCCUSL has significantly scaled back the draft UETA. The working group of experts, which includes private sector experts as well as public sector members, has reached general agreement that the UETA should enable electronic signatures as a major step toward removing existing legal barriers to electronic commerce; it has removed all references to elements of "trustworthiness" and associated presumptions. See "NCCUSL Significantly Changes Focus of Uniform Electronic Transactions Act", ITEC Law Alert Vol. 8, No. 3, June 1998, www.mbc.com/newsin83.html. The UNCITRAL Model Law has been the basis for much of this work. It is expected that a final draft will be issued by the end of summer 1999**.** The United States recognises published criteria, the observance of which renders electronic documents or signatures admissible for evidentiary purposes. The general principle is found in Federal Rule of Evidence 1001, which allows electronic records to be considered both "writings" and "originals". There is no central public body in the US that issues digital certificates for general public use. A number of private companies offer such services, either directly or as suppliers. A general survey of the electronic delivery of government services at the federal level can be found at: http://www.gits.gov/htm/access.htm. A more detailed survey of issues related to security (including authentication) in the provision of government services electronically can be found in the report, "Access with Trust", at: http://gits-sec.treas.gov/. It is impossible to count the number of efforts underway by the US private sector. Examples of public sector efforts are identified above. There are a variety of models in operation and under development in the US. A model could be found in virtually every sector of the economy, from financial services to manufacturing, from services to retail.

Private contractual agreements

US Law, at both the federal and state level and at the state level, respects private contractual agreements concerning the use and recognition of electronic signatures. Parties are free to agree to standards, procedures for themselves. US law, on the whole, does not set forth specific standards and procedures in the area of electronic signatures. Parties may seek to have their contractual arrangements enforced in US courts of law. No unique evidentiary standards apply to the use of electronic signatures under US law.

Standards

A number of private sector standards bodies have been active in the area of electronic authentication, most notably in the ANSI X.9. There are no laws, regulations or private sector mechanisms governing or developing/setting standards for digital signatures, electronic signatures, or other kinds of electronic authentication, and no US law makes compliance with standards in this area mandatory. The US private sector plays the lead role in developing and implementing standards for digital signatures. As noted above, there are no legislatively or administratively approved standards at the national level in this area. Generally, compliance and certification with respect to any standard is done by the private sector.

Certification authorities

As noted above, a variety of private sector initiatives is underway. It would be expected that any issues related to "accrediting" or operating the issuance of digital certificates would be addressed by those private sector frameworks. The requirements for a certification authority, to the extent they exist, vary based on the industry sector needs and business model employed. As a general matter, US policy and law recognises the key role played by private sector accreditation schemes. No unique set of liability rules apply to the activities of certification authorities in the US.

Global authentication

US law recognises digital signatures and other kinds of electronic authentication used in other countries where parties to a transaction or business system identify such technologies or implementations. US law does not extend to providers of "trusted services". Moreover, the concept of "trusted service provider" does not have a direct analogy to US experience. No central public authority that will cross-certify certification authorities at the national or sub-national level exists. Where a need is identified in a particular sector of business or industry, appropriate private sector bodies undertake such efforts. There are active exchanges of information between these private sector initiatives and governmental agencies. In most (if not all) private sector models, the issue of "cross-certification" is not raised since once a closed system operates on a global basis the issue is moot.

National Contact Points

Inquiries may be directed to:
Mark Bohannon
US Department of Commerce
Tel: +1 202 482-1984 (Voice)
Tel: +1 202 482-0253 (Fax)
E-mail: Mark_Bohannon@ta.doc.gov

ACTIVITIES AT THE INTERNATIONAL LEVEL

Private Sector Policy Initiatives

- *General Usage for International Digitally Ensured Commerce*[38] *(GUIDEC),* International Chamber of Commerce, Electronic Commerce Project, 1997. The GUIDEC was drafted by the ICC as part of its Electronic Commerce Project to help provide a basis of definitions and best practices to facilitate the development of a global framework for the "ensuring" of commerce over electronic media.

- *The Role of Certification Authorities in Consumer Transactions*, Working Group On Certification Authority Practices, Internet Law and Policy Forum, (ILPF) [39], 14 April 1997.

- *Trans-Atlantic Business Dialogue (TABD).*

Public Sector Activities

- *Model Law on Electronic Commerce*, United Nations Commission on International Trade Law (UNCITRAL), 1996.[40] Following the Model Law, the UNCITRAL Working Group on Electronic Commerce currently has work underway regarding the legal aspects of electronic commerce: digital signatures, electronic signatures certification authorities and related legal issues.

- *Communication on Ensuring security and trust in electronic communication - towards a European framework for digital signatures and encryption*, European Commission, (COM(97) 503), October 1997. The Communication describes both the authentication and integrity functions of cryptography, as well as confidentiality functions. The Communication advocates international action to create a framework for electronic commerce that would involve mutual recognition of certificates and common technical standards. It also addresses a variety of issues related to the use of cryptography for encrypting data.

- *Proposal for a European Parliament and Council Directive on a common framework for electronic signatures*, European Commission, (COM(1998) 297 final, 13.05.98)[41]. The proposed Directive follows the Communication, with a view to harmonising European

38. See http://www.iccwbo.org/guidec2.htm.

39. See http:// www.ilpf.org.

40. See http:www.un.or.at/uncitral/index.html.

41. See http://www.ispo.cec.be/policy.

initiatives on electronic signatures and to promoting the legal recognition of electronic signatures. The proposal also contains provisions for cross-border mechanisms aimed at ensuring interoperability at a global level. It is currently under consideration by the European Parliament and Council.

- *Enabling global electronic commerce through compatible postal trust services: building trust for users and consumers*, Universal Postal Union (UPU), International Bureau, Postal Technology Centre, 1997-1998.

- *Public Key Authentication Task Group Preliminary Report*, Asia Pacific Economic Cooperation (APEC), Telecommunications Working Group, Business Facilitation Steering Group, September 1997.[42]

- *Recommendation of the OECD Council concerning Guidelines for Cryptography Policy*, Organisation for Economic Co-operation and Development, March 1997.

- *Initiative on Information Security Standards*, Open Information Interchange (OII), INFO 2000 programme, European Commission DG XIII.

- *Secure Electronic Authentication Linkages (SEAL) Program*, and the Certification Authority Test Plan, United Nations Conference on Trade and Development, United Nations Trade Point Documentation Centre, 1998.

- *Copenhagen Hearing on Digital Signatures*, Danish Ministry of Research and Information Technology, European Commission DG XIII, 3 July 1998.[43]

Technical Standards Development Initiatives

- *Digital Signature Initiative (Dsig)*, World Wide Web Consortium (W3C) DSIG 1.0 Proposed Recommendation, for review November 1997, January 1998.[44] This project aims to use digital signature, certificate and meta-data technologies to provide a comprehensive solution to the basic problems of helping users decide what to trust on the Web, by defining effective ways to represent digitally signed assertions and endorsements, extending beyond identity and integrity functions.

- *Guidelines for Use and Management of Trusted Third Parties*, Proposed Draft Technical Report, for Review and Comment, Information Technology Security Techniques, ISO/IEC JTC 1/SC 27 PDTR, International Standards Organisation, 27 May 1997. A meeting was held on 20–24 April 1998 to examine this draft. A new draft was presented during summer 1998, which will be put for a vote in the coming months.

42. See http://www.apecsec.org.sg/telewg/16tel/bfsg/matrix/TELEWG-BFSG-3e-2.html.

43. See http://www.fsk.dk/fsk/div/hearing.

44. See http://www.w3c.org/pub/WWW/Security/DSig/.

- *Glossary of IT Security Terminology*, SD6, SC 27 N 1954, International Standards Organisation, 5 March 1998.

- *European Telecommunications Standards Institute (ETSI)* work on key management and electronic signatures. The ETSI TC Security Group has been working on a set of standards for key management (with or without escrow), authentication, notarisation and other services. Part I of this standard went out for public comment earlier this year and failed to gain sufficient support from member states. Further work on key management has been halted till 1999. ETSI continues its work on proposals for standardisation of electronic signatures, to investigate what exists already, identify gaps and overlaps, and determine the appropriate role for ETSI.

SUMMARY TABLES : COUNTRY ANSWERS TO THE QUESTIONS FOR FRAMING FURTHER INPUT TO AUTHENTICATION INVENTORY AND UPDATE ON DEVELOPMENTS IN THIS AREA

General Questions	Have steps been taken, where appropriate, to favourably take account of the 1996 UNCITRAL Model Law on E-Commerce in relevant national laws or policies?	**Does the Country have:**		
		a specific national law or regulation concerning digital or electronic signatures, or other kinds of electronic authentication?	**any set criteria, observance of which render electronic documents or signatures admissible in evidence?**	**a public or private sector body which issues digital signatures for public use?**
AUSTRALIA	In preparation	In preparation	No	Yes
AUSTRIA	In preparation	In preparation	In preparation	In preparation
BELGIUM	No	In preparation	No	Yes
CZECH REP.	Yes	No	No	Yes
FINLAND	Yes	No	No	No
GERMANY	In preparation	Yes	N/A	Yes
GREECE	No	No	No	No
JAPAN	No	No	N/A	No
MEXICO	Yes	No	No	Yes
NETHERLANDS	No	No	No	Yes
NEW ZEALAND	Yes	No	Yes	Yes
NORWAY	Yes	No	No	Yes
POLAND	Yes	No	No	No
SWEDEN	Yes	No	No	Yes
TURKEY	No	No	No	No
UK	Yes	No	No	Yes
US	Yes	No	Yes	Yes

General Questions	Are authentication technologies or mechanisms used in the delivery of Government services to citizens?	Are any national initiatives, studies, proposed legislation or rules underway or under consideration in the area of authentication and certification?	Are there any private sector models for electronic authentication in operation or under development?
AUSTRALIA	In preparation	Yes	Yes
AUSTRIA	In preparation	Yes	In preparation
BELGIUM	No	Yes	Yes
CZECH REP.	No	Yes	Yes
FINLAND	No	Yes	Yes
GERMANY	Yes	-	Yes
GREECE	No	Yes	No
JAPAN	No	Yes	Yes
MEXICO	Yes	Yes	Yes
NETHERLANDS	No	Yes	Yes
NEW ZEALAND	Yes	No	No
NORWAY	Yes	Yes	Yes
POLAND	No	Yes	Yes
SWEDEN	Yes	Yes	Yes
TURKEY	No	Yes	Yes
UK	Yes	Yes	Yes
US	Yes	Yes	Yes

Private Contractual Agreements	**Does national law or regulation on private contractual agreements limit the use and recognition of digital or electronic signatures, or other kinds of electronic authentication?**	**Are parties free to agree to standards, procedures, and uses that differ from those set forth in national laws and regulations?**	**If the parties use different standards from national laws or regulations, may they still use the national legal system to attempt to gain redress under the contract?**	**Do evidentiary standards apply to evidence of validity and authenticity offered to national judicial or administrative proceedings?**
AUSTRALIA	No	Yes	Yes	No
AUSTRIA	No	Yes	Yes	No
BELGIUM	No	Yes	Yes	No
CZECH REP.	No	Yes	Yes	No
GERMANY	No	Yes	Yes	Yes
GREECE	No	Yes	Yes	No
JAPAN	No	Yes	Yes	No
MEXICO	No	Yes	Yes	No
NETHERLANDS	No	Yes	Yes	Yes
NEW ZEALAND	In preparation	Yes	Yes	No
NORWAY	No	Yes	Yes	No
POLAND	No	Yes	Yes	No
SWEDEN	No	Yes	Yes	No
TURKEY	No	Yes	Yes	No
UK	No	Yes	N/A	No
US	No	Yes	Yes	No

Technology Requirements	**Does national law or regulation specifically approve a particular kind of electronic authentication technology or mechanism?**	**Does national law or regulation preclude or disadvantage a party using an authentication method other than one specifically approved?**	**Can parties using authentication methods not directly approved by national law or regulation establish its method's validity by offering evidence of reliability in judicial or administrative proceedings?**	**Does national law or regulation identify certain electronic authentication technology as "secure"?**
AUSTRALIA	No	N/A	N/A	No
AUSTRIA	No	N/A	N/A	No
BELGIUM	No	N/A	N/A	No
CZECH REP.	No	N/A	N/A	Yes
FINLAND	No	N/A	Yes	No
GERMANY	Yes	No	Yes	No
GREECE	No	N/A	N/A	No
JAPAN	No	N/A	N/A	No
MEXICO	No	N/A	N/A	No
NETHERLANDS	No	N/A	N/A	No
NEW ZEALAND	No	N/A	N/A	No
NORWAY	No	N/A	N/A	No
POLAND	No	N/A	N/A	No
SWEDEN	No	N/A	N/A	No
TURKEY	No	N/A	N/A	No
UK	No	N/A	N/A	No
US	No	N/A	N/A	No

Technology Requirements	Does national law or regulation differentiate between levels of security?	Does national law or regulation set forth technical requirements for components or systems used in electronic authentication?	Do national laws or regulations require technical components of systems used in electronic authentication to be accredited or licensed?	What are the consequences in proceedings of using an alternative to legislatively or administratively approved methods of electronic authentication?
AUSTRALIA	No	No	No	N/A
AUSTRIA	No	No	No	N/A
BELGIUM	No	No	No	N/A
CZECH REP.	Yes	No	No	N/A
FINLAND	No	No	No	In preparation
GERMANY	Yes	Yes	Yes	No “security” presumption
GREECE	No	No	No	N/A
JAPAN	No	No	No	N/A
MEXICO	No	No	No	N/A
NETHERLANDS	No	No	No	N/A
NEW ZEALAND	No	No	No	N/A
NORWAY	No	No	No	N/A
POLAND	No	No	No	N/A
SWEDEN	No	No	No	N/A
TURKEY	No	No	No	N/A
UK	No	No	No	No auto-presumption of proof
US	No	No	No	N/A

Standards	Have national or sub-national standards for electronic authentication been developed by the public or private sectors?	Do national laws, regulation or private sector mechanisms govern or develop the setting of standards for electronic authentication?	Is compliance with any standards in the field of electronic authentication mandatory?	Could failure to follow specified standards lead to liability in civil proceedings or increase the chance a party will be held liable for using an alternative standard?
AUSTRALIA	Yes	Yes	No	No
AUSTRIA	No	No	No	No
BELGIUM	No	No	No	No
CZECH REP.	No	No	No	No
FINLAND	Yes	Yes	No	No
GERMANY	Yes	Yes	No	No
GREECE	No	No	No	No
JAPAN	Yes	Yes	No	No
MEXICO	Yes	No	Yes	-
NETHERLANDS	No	Yes	No	No
NORWAY	Yes	Yes	No	No
POLAND	No	No	No	No
SWEDEN	Yes	No	No	No
TURKEY	Yes	No	-	-
UK	No	Yes	No	No
US	Yes	No	No	N/A

Standards	Does the private sector play a role in developing and certifying standards for digital signatures, electronic signatures or other kinds of electronic authentication?	Do national laws or regulations permit private-sector bodies to certify compliance with legislatively – or administratively approved standards?	What national private sector initiatives exist concerning standards and related issues in the area of authentication?
AUSTRALIA	Yes	No	Standards Australia, Certification Forum of Australia
AUSTRIA	No	No	N/A
BELGIUM	Yes	Yes	Agora Project, Belgacom, Publilink, Isabel, Belsign.
CZECH REP.	Yes	No	-
FINLAND	Yes	Yes	Merita Nordbanken
GERMANY	Yes	Yes	DIN German National Standardisation Body
GREECE	No	No	ACCI – Pilot Certification Authority
JAPAN	N/A	N/A	Guidelines produced on matters including cross-certification
MEXICO	Yes	No	Private sector participation in NOM 157
NETHERLANDS	Yes	Yes	TTP.NL – concerns standards of authentication
NORWAY	Yes	-	-
POLAND	Yes	No	Banking Sector working on Standard of Authentication
SWEDEN	Yes	Yes	Secured Electronic Information in Society Association
TURKEY	Yes	-	-
UK	Yes	Yes	Alliance for Electronic Business
US	Yes	No	

Certification Authorities	**Are any measures being taken to evaluate and approve, or accredit, certification authorities or other providers of trusted services?**	**Do national laws or regulations set requirements for licensing or accrediting "certification authorities"?**	**Are there private sector models for accreditation of certification authorities in operation or under development?**	**Do national laws or regulations have mechanisms to recognise private sector accredited entities?**
AUSTRALIA	Yes	No	Yes	No
AUSTRIA	In preparation	In preparation	In preparation	In preparation
BELGIUM	Yes	No	Yes	No
CZECH REP.	In preparation	In preparation	In preparation	In preparation
FINLAND	No	No	No	No
GERMANY	Yes	Yes	Yes	No
GREECE	In preparation	No	No	No
JAPAN	Yes	N/A	Yes	N/A
MEXICO	Yes	No	No	No
NETHERLANDS	Yes	No	Yes	No
NEW ZEALAND	Yes	No	No	No
NORWAY	Yes	No	No	No
POLAND	Yes	No	No	No
SWEDEN	Yes	No	No	No
TURKEY	No	No	No	No
UK	Yes	No	Yes	No
US	Yes	No	Yes	Yes

Certification Authorities	Do legal or regulatory requirements which govern regulation and accreditation of certification authorities, vary by sub-national jurisdiction?	Are there any national proposals to limit the liability of certification authorities?	What national liability rules currently apply to the activities of certification authorities?
AUSTRALIA	No	No	Normal commercial liability rules apply.
AUSTRIA	In preparation	In preparation	In preparation.
BELGIUM	No	No	Common law rules, law in preparation sets min and max.
CZECH REP.	In preparation	No	No explicitly defined liability rules.
FINLAND	No	No	-
GERMANY	No	No	No specific liability rules apply.
GREECE	No	Yes	Can be liable for defective info. in certificate if negligent.
JAPAN	N/A	No	Normal Civil Law applies.
MEXICO	No	No	-
NETHERLANDS	No	No	Normal Civil Code Rules apply.
NEW ZEALAND	No	No	Normal commercial contractual obligations apply.
NORWAY	No	Yes	-
POLAND	No	No	-
SWEDEN	No	No	Normal tort law applies.
TURKEY	No	No	-
UK	No	In preparation	-
US	N/A	No	-

Global Authentication	Do national laws or regulations recognise digital signatures, electronic signatures or other kinds of electronic authentication used in other countries?	If national laws or regulations govern providers of trusted services related to electronic authentication, are there procedures to recognise foreign providers of similar services?	Do national laws or regulations place limitations on cross-border recognition of electronic authentication?	Is there a central public or private sector body that will cross-certify certification authorities at the national or sub-national level?
AUSTRALIA	Yes	N/A	No	No
AUSTRIA	In preparation	In preparation	In preparation	In preparation
BELGIUM	In preparation	In preparation	In preparation	In preparation
CZECH REP.	No	No	No	No
FINLAND	Yes	No	No	No
GERMANY	Yes	Yes	Yes	No
GREECE	No	No	No	No
JAPAN	N/A	N/A	N/A	N/A
MEXICO	Yes	N/A	No	No
NETHERLANDS	No	No	No	No
NEW ZEALAND	No	N/A	No	No
NORWAY	Yes	No	No	Yes
POLAND	No	No	No	In preparation
SWEDEN	Yes	No	No	No
TURKEY	No	No	No	No
UK	Yes	Yes	No	Yes
US	Yes	N/A	No	Yes

Global Authentication	Where national cross-certification procedures are in place, do they vary by sub-national jurisdiction?	Are there private sector models for cross-certification of certification authorities?	Do national laws or regulations place limitations on cross-certification between certification authorities operating in different countries?
AUSTRALIA	N/A	No	No
AUSTRIA	In preparation	In preparation	In preparation
BELGIUM	In preparation	In preparation	In preparation
CZECH REP.	N/A	No	No
FINLAND	N/A	No	No
GERMANY	N/A	Yes	Yes
GREECE	N/A	No	No
JAPAN	N/A	N/A	N/A
MEXICO	N/A	No	No
NETHERLANDS	No	Yes	No
NEW ZEALAND	No	No	No
NORWAY	No	Yes	No
POLAND	No	Yes	No
SWEDEN	No	No	No
TURKEY	No	No	No
UK	No	Yes	No
US	N/A	N/A	No