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

16-Sep-2002

English - Or. English

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

DSTI/ICCP/REG(2001)10/FINAL
Unclassified

Working Party on Information Security and Privacy

PROGRESS ACHIEVED BY OECD MEMBER COUNTRIES IN FURTHERANCE OF THE OTTAWA DECLARATION ON AUTHENTIFICATION FOR ELECTRONIC COMMERCE

JT00131509

English - Or. English

EXECUTIVE SUMMARY

The Declaration on Authentication for Electronic Commerce (the "Declaration"), adopted by Ministers at the Ottawa Ministerial Conference on 7-9 October 1998, recognised the importance of authentication for electronic commerce. It outlined a number of actions to promote the development and use of electronic authentication technologies and mechanisms, including continuing work at the international level, together with business and industry representatives, as well as users.

A Steering Group was established by the Working Party for Information Security and Privacy (WPISP) in order to prepare a report on progress made with regard to implementing the Declaration, including initiatives developed and results achieved in member countries. The Steering Group examined how national policies and laws are currently implemented, and has conducted a survey on form requirements, which have been identified as potentially major obstacles to the implementation of electronic authentication and electronic commerce.

The study was conducted for each item of the issues that the Declaration addressed.

As for **the legal recognition of electronic signatures**, the progress after the October 1998 Ottawa Declaration is evident. Most of the member countries have already amended technology or media-specific requirements in current laws or policies, where appropriate, and have given legal recognition to electronic signatures. Most of the other member countries either have drafts of amendments ready or work is underway. We might encourage continuing efforts in those countries that are preparing for legislation.

As for **giving favourable consideration to the UNCITRAL Model Law**, clauses of the UNCITRAL Model Laws such as "legal recognition", "variation by agreement" and "court admissibility" are commonly reflected in national legislation or regulation where amendments were made. It might be necessary to encourage continuing efforts in those countries that are preparing for legislation.

As for a **non-discriminatory approach to foreign authentication**, governments either express policies for non-discrimination, or remain silent about nationality of authentication, which is interpreted as being non-discriminatory to foreign authentication. However, the differences in standards or schemes among countries cause certain concern for the interoperability of electronic signatures and cross-certification of CAs. There seems to be a need for compatibility of approaches and policies among OECD member governments and business initiatives for the purpose of establishing international real marketplace interoperability of electronic authentication systems.

As for **encouraging efforts to develop and facilitate the use of authentication technologies,** form requirements are still found in many aspects of commercial activities, including those areas the survey covered. Remaining form requirements are apparent and pose challenges for governments to tackle.

As for **applying authentication technologies to the delivery of government services,** developments in this area are encouraging, in that almost all the member governments either have started initiatives to introduce electronic measures to be used in government services, or have plans to do so. Some governments explicitly reported their intention to accept only "secure" electronic signatures in transactions with the government. This may not cause specific problems with the objective of promoting electronic services in their systems, but may justify further efforts to establish the interoperability of electronic authentication internationally.

As for **continuing work at the international level**, it is important to note that in many member countries, legal systems promoting the usage of electronic means are still being developed. There is no reason to assume these changes have lost their momentum at this stage.

This report contains the Steering Group's findings on progress in the implementation of the Declaration including initiatives developed and results achieved in member countries. It is important to note that in many member countries, approaches to authentication and certification on global networks, including laws, policies and initiatives are still being developed in light of evolving technologies and in consideration of works at international level. Therefore it would be useful to have a more in-depth review of the developments, especially its implication to cross-border issues related to form requirements when the follow-up activities of this review are carried out.

TABLE OF CONTENTS

PROGRESS ACHIEVED BY THE OECD MEMBER COUNTRIES IN FURTHERANCE OF THE OTTAWA DECLARATION ON AUTHENTICATION FOR ELECTRONIC COMMERCE

CONTEXT

The Ottawa Declaration on Authentication for Electronic Commerce

The Declaration on Authentication for Electronic Commerce adopted by Ministers at the Ottawa Ministerial Conference on 7-9 October 1998[1] recognised the importance of authentication for electronic commerce. It outlined a number of actions to promote the development and use of electronic authentication technologies and mechanisms, including continuing work at the international level, together with business, industry and user representatives.

In the Declaration, Ministers declared their determination to:

- Take a non-discriminatory approach to electronic authentication from other countries.
- Encourage efforts to develop authentication technologies and mechanisms, and facilitate the use of those technologies and mechanisms for electronic commerce.
- 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 Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996.
- Proceed with the application of electronic authentication technologies to enhance the delivery of government services and programmes to the public; and
- Continue work at the international level, together with business, industry and user representatives, concerning authentication technologies and mechanisms to facilitate global electronic commerce.

Preparation of a report on progress achieved by the OECD in furtherance of the Ottawa Declaration on Authentication for Electronic Commerce

Following the Declaration, a joint OECD-Private Sector Workshop on Electronic Authentication was held in Stanford, California, in June 1999[2], with discussions on the emerging technologies, models and issues for authentication. The workshop looked at the range of possibilities in technologies and models for electronic authentication, as well as the public policy issues in this area. In addition to active private sector participation, the APEC Telecommunications Working Group also participated. The workshop was one of the follow-ups of the Ottawa Declaration in that the governments "continue work at the international level, together with business, industry and user representatives, concerning authentication technologies and mechanisms to facilitate global electronic commerce."

1. OECD Ministerial Conference "A Borderless World: Realising the Potential of Global Electronic Commerce", 7-9 October 1998 SG/EC(98)14/FINAL, http://www.olis.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)14-final.

2. http://www.oecd.org/dsti/sti/it/secur/act/wksp-auth.htm

Following the workshop, the Working Party on Information Security and Privacy (WPISP) decided to set up a Steering Group to prepare a report on progress in the implementation of the declaration including initiatives developed and results achieved in member countries.

The Steering Group was established and examined how national policies and laws are currently implemented with regard to facilitating legal recognition, party autonomy, technology neutrality, global authentication mechanisms and user confidence, and ensuring that there is no legal discrimination in relation to different types of authentication technology. To this end, the Steering Group has revised *the Inventory on Authentication and Certification in a Global Networked Society [DSTI/ICCP/REG(99)13/FINAL]* and has conducted a survey on form requirements, which have been identified as potentially major obstacles to the implementation of electronic authentication and electronic commerce.

In conducting a survey on form requirements, a questionnaire *(attached as Annex 2)* was developed under the auspices of the Steering Group members, and then circulated among member governments. Analysis in this area needed to be targeted to avoid a scope of work too broad to be accomplished with the one-year time frame provided. While the outcome of this work is meant to be useable across sectors, the initial inquiry focused on four main areas for the following reasons:

- Financial services: Banking and brokerage, early adopter of authentication, highly regulated sector, commercial and consumer.
- Transport: Intersection of virtual and real worlds (hybrid transactions), cross-border form requirements, commercial and consumer application.
- Government to B/C: How governments interact with citizens and industry is of critical importance — crossover from/to e-services, benchmark for implementation of Ottawa principles.
- Commercial contracting: Broader look at e-contracting issues with paradigms from other sectors and ability of parties to determine contractual appropriateness.

In addition, the Steering Group continually collected information on the activities of APEC economies in this area through member delegates acting as liaisons to APEC.

This report contains the Steering Group's findings on progress in the implementation of the declaration including initiatives developed and results achieved in member countries, as well as recommendations to government and business as a result of the Steering Group's findings. It is important to note that in many member countries approaches to authentication and certification on global networks, including laws, policies and initiatives are still being developed, in light of evolving technologies and in consideration of works at international level. Therefore it would be useful to have a more in-depth review of the development, especially its implication to cross-border issues related to form requirements when the follow-up activities of this review are carried out.

PROGRESS ACHIEVED BY THE OECD MEMBER COUNTRIES IN FURTHERANCE OF THE OTTAWA DECLARATION ON AUTHENTICATION FOR ELECTRONIC COMMERCE

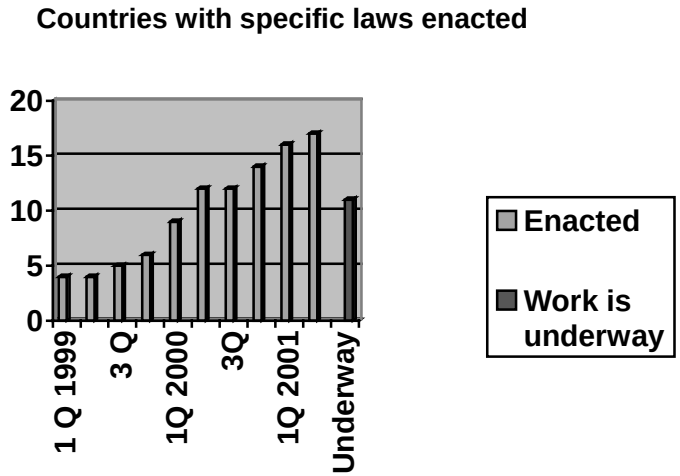
1. Legal recognition of electronic signatures

Declaration: "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"

Findings

Although the revised Inventory (*the Inventory on Authentication and Certification in a Global Networked Society)* shows a static "snapshot" of policy developments in member governments, when we compare the contents with the previous Inventory issued in 1999 *[DSTI/ICCP/REG(99)13/FINAL]*, a dynamic view can be obtained.

In 1999, six member countries reported that they had enacted/modified specific legislation to give legal recognition to electronic signatures. One year later, the number of countries that had adopted specific laws had increased to 17.



Notably, EU member countries are now in the process of implementing the EU Directive on Electronic Signatures[3]. The EU Directive entered into force on 19 January 2000 and has to be implemented by the EU member countries by 19 July 2001. As a result, all 15 EU member countries have passed new legislation, amended legislation or are drafting legislation for the implementation of the Directive. In addition, three

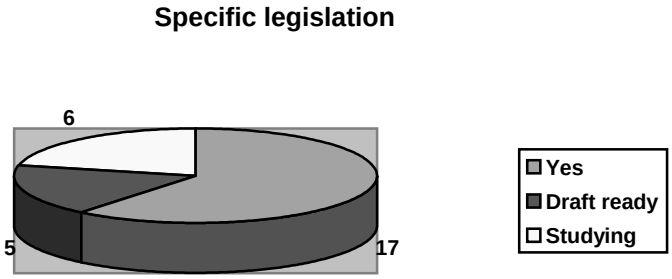
3. European Parliament and Council Directive, 1999/93/EC of 13 December 1999 on "A Community Framework for Electronic Signatures", OJ No L 13 p.12 19/1/2000.

non-EU member countries, the Czech Republic, Hungary and Norway, reported that they are drafting legislation in compliance with the EU Directive.

The EU Directive harmonises national approaches with regard to electronic authentication and aims to strengthen user confidence in electronic communication. The Directive aims to contribute to the legal recognition of electronic signatures. It establishes a legal framework for electronic signatures and certain certification services in order to ensure the proper functioning of the EU internal market. The Directive also contains provisions for cross-border mechanisms aimed at ensuring interoperability at a global level[4].

In other non-EU member countries, Australia, Canada, Japan, Korea, Switzerland and the United States reported the introduction of specific laws or amendments to existing laws to give legal recognition to electronic signatures. Iceland, Mexico, Poland and Turkey reported that work or review is underway in this area.

In total, among the 11 countries that have not enacted specific laws, five responded that either a draft is ready or a draft is now before parliament. The other six responded that either work or a study is underway, or that a review of existing laws is underway.



Observations

The progress after the October 1998 Ottawa Declaration is evident. In total, 17 member countries, not only EU member states, have amended technology or media-specific requirements in current laws or policies, where appropriate, and have given legal recognition to electronic signatures. Most of the other member countries either have drafts of amendments ready or have begun work. See Annex 3 for further information.

We might encourage continuing efforts in those countries that are preparing for legislation. We also might consider providing outreach with regard to these activities to OECD non-member countries.

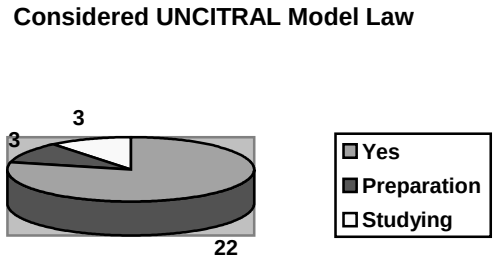
4. Article 7 of the EU Directive on Electronic Signatures specifies the condition under which certificates issued by a certification service provider established in a third country are recognised as legally equivalent to certificates issued within the Community. They are: *(a)* the certification service provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a member state; or *(b)* a certification service provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or *(c)* the certificate or the certification service provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

2. Favourable consideration to UNCITRAL Model Law

Declaration: "give favourable consideration to the relevant provisions of the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996"

Findings

Of the 28 countries that responded to the survey on the Inventory, 22 responded that they have given favourable consideration to the UNCITRAL Model Law. Most of the consideration came in the process of



amending legislation or regulations. This number is larger than the number of countries that have enacted specific laws on electronic signatures. Countries that have considered the UNCITRAL Model Law during the process of drafting laws are counted even if those laws have not yet been enacted. Of those six countries that have not yet considered the UNCITRAL Model Law, three responded that they now are preparing legislation, and the other three responded that work/study is underway.

Although a detailed examination of the extent to which such consideration was paid was not included in the questions for the Inventory, it is commonly observed that "legal recognition", "variation by agreement" and "court admissibility" are the areas in which legislation has followed the UNCITRAL Model Law.

Of those 28 countries that responded, 27 countries said that parties are free to agree on standards, procedures and uses of electronic signatures. One country did not supply specific information as to this point, but did not necessarily signal a negative response. Likewise, 27 countries allowed electronic signatures that parties chose to use to be admissible in court. Notably, these responses suggest that even without the introduction of specific laws on electronic signatures, civil code or free evidential principles are being applied to them.

In some cases, countries supplied additional information relating to the Model Law. According to this information, some reservation with regard to the "attribution" or "acknowledgement of receipt" clause of the Model Law was observed in at least one case (Australia).

Observations

Clauses of the UNCITRAL Model Laws such as "legal recognition", "variation by agreement" and "court admissibility" are commonly reflected in national legislation or regulation where changes took place. There was, however, a case of explicit reservation with regard to some clauses like "attribution" or "acknowledgement of receipt". As the present survey does not include a detailed examination of these

issues, a detailed survey of the applicability of each clause of the Model Law would need to be conducted if it were a concern.

However, it might be more constructive to encourage continuing efforts in those countries that are preparing legislation, and we might also consider providing outreach to OECD non-member countries in order to encourage further adoption of the Model Law.

3. Non-discriminatory approach to foreign authentication

Declaration: "take a non-discriminatory approach to electronic authentication from other countries"

Findings

No government pursues policies to explicitly discriminate against foreign authentication. In some cases, legislation or regulations are silent about the treatment of foreign authentication. Even in those cases, silence in laws is regarded as a sign that no additional burdens are required for foreign authentication. But in determining "secure" electronic signatures or "qualified" electronic signatures", there may be differences in criteria among countries, and even though those criteria are equally applied to domestic and foreign authentication, differences among the countries themselves might cause some concern. As an example, in the EU Directive, in order for an electronic signature to be "qualified", there are general requirements for certification services providers (Annex 2 of the EU Directive), and for signature creation devices (Annex 3 of the EU Directive). Among EU member countries, interoperability of authentication for "qualified" electronic signatures is envisaged, but the details of the system to assure interoperability would need to be developed further. In addition, interoperability with systems other than those based on the EU Directive is yet to be developed.

Although such requirements for signatures to be "secure" or "qualified" are usually generic in their expression, in practice, their interpretation might differ depending on systems, and details of these requirements are, in most cases, under development. The use of "secure" signatures is not mandatory, except where required for transactions with governments. The differences in the requirements among different systems might be a potential cause of concern for those involved in the international exchange of electronic signatures.

Where certification authorities (CAs) are accredited by governments, there may be requirements of financial viability, technical reliability and record keeping. Although in many cases the details of accreditation schemes are as yet to be determined, differences in requirements might be a potential cause of concern. There was no country that conditioned specific nationality of the CA to be accredited, but there was a case (Australia) where physical presence within the territory was required for the provision of services to government. In order to achieve mutual acceptance of the certificates issued by the CA, mutual agreements between the governments are referred to as options in some cases (Japan, Korea).

In the EU regime, attention should be paid to the activities of the EESSI (European Electronic Signature Standardisation Initiative[5]). The EU Directive identifies minimal requirements for certificates, certification service providers and signature creation and verification devices. The Directive allows the Commission to establish and publish references of generally recognised standards for electronic signature products. As a consequence, member states' laws shall presume compliance with the requirements laid down in the Directive when a product meets those standards. The European ICT Standards Board, with the support of

5. EESSI (European Electronic Signature Standardisation Initiative): http://www.ict.etsi.org/eessi/EESSI-homepage.htm

the European Commission, has launched an initiative, EESSI, bringing together industry and public authorities, experts and other market players. EESSI seeks to identify the needs for standardisation activities in support of the Directive's requirements, and to monitor the implementation of the work programme under a common approach. EESSI provided a first set of deliverables to the European Commission on 3 April 2001 that contained four ETSI standards "ETSI TS 101 465: Policy Requirement for Certification Authorities Issuing Qualified Certificates", "ETSI TS 101 862: Qualified Certificate Profile", "ETSI TS 101 861: Time Stamping Profile" and "ETSI TS 101 733: Electronic Signature Formats."[6]

In Nordic countries (Finland, Norway and Sweden), discussions have started with SWEDAC, the Swedish Board for Accreditation and Conformity Assessment, about the international use of the SWEDAC-SAT (Self-Assessment Test) testing tool[7]. SWEDAC-SAT is a test tool for verifying certificates and certificates on smart cards (electronic ID cards). It consists of two parts: one for verifying certificates and one for verifying electronic ID cards. It checks that the certificate and the electronic ID cards have the correct filing system and format, as defined in the applicable standards. Testing of the certificates and cards ensures that the cards can be used in the same way by different applications. The tool ensures interoperability between different types of systems. In 2000, there was a plan to upgrade the tool to be based on the European and international standard for electronic signatures. The tool would be based on an upgraded specification of the test specification and was due to be implemented in the spring of 2001.

APEC activities have been continuously reported to the Steering Group through members (Australian Delegates and Canadian Delegates) acting as a liaison to APEC activities. The APEC telecommunication working group and its PKI Interoperability Experts Group recently discussed a proposal to carry out a project that would assist member economies in identifying and mapping the certification authority and accreditation linkages that are necessary for organisations to securely interact and transact with each other electronically across jurisdictional boundaries.[8] Even among APEC economies, it is recognised that there are differences in some of the approaches being taken. The value in the project is that it will facilitate a pulling together of the different approaches and provide for an analysis of how the variances might be adapted to meet the same objectives. This could lead to interoperable e-commerce across the region. It is already becoming apparent that different business models have emerged and the criteria critical to an assessment of a certificate's trust may appear in different locations. This mapping exercise is expected to encourage and facilitate real marketplace interoperability by highlighting commonalties and, moreover, recognising where differences need to be addressed.

Although there are differences in laws on electronic signatures and involvement in the government centred CA accreditation schemes between the two countries, a Canada-US PKI Liaison Group has been formed to promote information exchange, collaboration and joint pilots between departments and agencies of the US and Canadian governments. It is expected to facilitate interoperability of different systems in the two countries.

It is important to note several other initiatives that have been launched at the national, regional and international levels. Activities at International Chamber of Commerce, the ILPF (Internet Law Policy

6. EESSI DDD (Deliverable Description Document) "EESSI First Set of Deliverables" (as given to the European Commission on 3 April 2001) http://www.ict.etsi.org/eessi/ddd.doc

7. For further information: http://www.swedac.se

8. APEC TEL Proposal "A Mapping of Certification Authorities Accreditation Schemes" by APEC Telecommunications Working Group - Business Facilitation Steering Group - Electronic Authentication Task Group - PKI Interoperability Experts Group; Tabled by Delegations of Canada and Singapore and reported to the OECD Steering Group on Authentication on 2 October 2000. ESTG/16 16.3.2001 23rd APEC TEL (http://www.tel23.org/Documents/estg/contact16.html.)

Forum), the IETF (Internet Engineering Task Force), and the ABA (American Bar Association) are among those that should be noted.

Observations

In order for electronic commerce to be conducted securely and efficiently across jurisdictions, electronic certification and authentication systems must be interoperable with one another, and cross-certification of CAs should be facilitated. For that purpose, a wider adoption and use of internationally operable electronic certification and authentication systems would greatly contribute to reducing the lack of reliability of, or the lack of trust in, electronic transactions. The international development and deployment of public key infrastructure (PKI) will create commercial incentives for vendors and users to bridge interoperability gaps between different PKIs. Third parties are beginning to offer bridging services and PKI vendors are looking at interoperability across policies, certificates and practices.

Even though the detailed legal systems for authentication and electronic signatures are under development in most of the member governments, in general, discrimination against foreign authentication in the strict sense may not be a major problem for interoperability among the countries based on responses to date. Governments either express policies for non-discrimination, or remain silent about nationality of authentication. However, the difference in standards or schemes among the countries cause certain concerns for interoperability of electronic signatures and cross-certification of CAs. There is also concern that there may be cases where cross-border form requirements may be neutral on the surface, but discriminatory in effect. Further attention should be paid to this eventuality.

As noted in the findings, regional studies, works, experiments and discussions are taking place among member and non-member countries as to the interoperability of their systems. The activities are not, however, sufficient to respond to the requirements of a wider international approach. An internationally consistent and coherent approach is necessary so that the legal framework for authentication and electronic signatures can build, as far as possible, upon standards or other forms of voluntary agreements, including business initiatives that would maximise their interoperability at the international level.

There seems to be a need for a compatibility of approaches and policies among OECD member governments and business initiatives for the purpose of establishing international interoperability of electronic authentication systems. Since the details of the schemes are still in development in most member countries, a framework for information exchange and study based upon initiatives of member countries and the private sector should be encouraged at an early stage, in particular so that the work can be reflected in the development of the systems internationally.

The work of UNCITRAL on Model Law on Electronic Signatures has been completed, and we may need to study its implications for our work[9].

To this end, member governments may wish to consider how global, seamless authentication and certification mechanisms should be developed through their support of UNCITRAL's work on Uniform Rules for electronic signatures as well as the OECD's work in this area.

9. The text of the UNCITRAL Model Law on Electronic Signatures was adopted by the United Nations Commission on International Trade Law at its 34th session, held in Vienna, 25 June - 13 July 2001. http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf

Options may include:

a) Developing a scheme following the APEC example in identifying and mapping the certification authority and accreditation linkages that are necessary for organisations to securely interact and transact with each other electronically across jurisdictional boundaries. It is recognised that there are differences in some of the approaches being taken. This project is expected to facilitate a pulling together of the different approaches and to provide for an analysis of how the variances might be adapted to meet the same objectives. This could lead to interoperable electronic authentication systems among member countries. From the experiences of the June 1999 joint OECD-Private Sector Workshop on Electronic Authentication in Stanford, it is apparent that different business models have emerged. This mapping exercise will help to encourage and facilitate real marketplace interoperability by highlighting commonalties and, moreover, recognising where differences need to be addressed.

b) Collecting and exchanging more detailed and specific information on some crucial aspects affecting interoperability of electronic certificates and authentication that have been identified in various previous studies. These may include (see EESSI activities in the previous section for more detail):

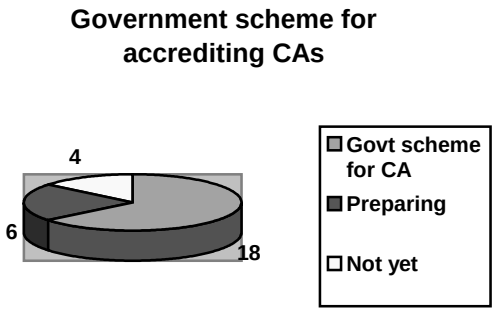
- Quality and functional standards for certification service providers.
- Quality and functional standards for signature creation and verification products.
- Interoperable standardisation requirements for electronic signatures.

This exercise will help to encourage and facilitate real marketplace interoperability by recognising where differences need to be addressed.

In carrying out these exercises, the "Web Trust System", a programme setting forth business best practices online and including an audit against compliance, might be a good example of a private sector initiative in this area.

4. Encourage efforts to develop and facilitate the use of authentication technologies

Declaration: "encourage efforts to develop authentication technologies and mechanisms, and facilitate the use of those technologies and mechanisms for electronic commerce"



Findings

Government accreditation schemes and voluntary/private initiatives exist. Some started with pilot projects for CAs. Central banks and post offices started services for specific purposes. Of the 28 countries that responded to the study, 18 countries responded that they have government accreditation scheme for CAs. Six others responded that they are either preparing or planning to establish a scheme. The remaining four countries currently have no plans in this area.

Form requirements were identified as potentially major obstacles to the implementation of electronic authentication and electronic commerce, and a survey was conducted to gather information on the issue.

In conducting a survey on form requirements, a questionnaire was developed under the auspices of Steering Group members, and then circulated among member governments *(Annex 2)*. The Steering Group has agreed that analysis in this area needed to be targeted in order to avoid too broad a scope of work to be accomplished within the provided timeframe. To this end, the survey was conducted on form requirements in the areas of "general commercial contracting", "financial services", "transportation and delivery services" and "delivery of government services".

In the area of government services, initiatives coupled with legislation on electronic signatures apparently have started. All of the 28 countries that responded to the survey reported the existence of some kind of plan, work or actual implementation in this area. Typically, some countries started with tax or VAT services via electronic means, either as a pilot project or actual implementation of legislation that enabled electronic transactions. Although an enormous amount of form requirements is observed in this area, the progress observed, and the general direction of developments, is encouraging.

In the area of electronic contracting, party autonomy on methods of contract, together with positive developments in legal recognition supplied by recent specific laws would further support and encourage usage of electronic means in contracting. Specific exceptions were observed in contracts for certain kinds of transactions such as real estate purchases, wills, adoption and divorce. However, they seemed to pose no serious problems for the promotion of electronic commerce.

In the area of financial services, mandatory form requirements still remain for certain transactions, such as written disclosures, hand-written signatures on bills and checks and written forms for consumer credit.

In the area of transportation and delivery services, in many cases form requirements were identified as originating from certain key international laws.

- **Montreal Protocol No. 4** (for air transport): The Protocol is not yet in force, but would allow for electronic signatures.
- **Hague-Visby Rules** (for Bills of Lading in international maritime, sea and ocean transport): The Hague Rules are the subject of two differing interpretations. Although there is a view that Article III would permit the shipper to specify that electronic data interchange (EDI) be used for the issuance of bills of lading, the majority view appears to be that the Convention envisages and requires paper bills of lading to be issued. Article III also refers to "writing" and "documents", which by implication includes written documents. The definition clause in the rules could be amended to state that a "document" is not restricted to paper.
- **Hamburg Rules:** The Hamburg Rules contain a non-exhaustive definition of "writing" to include telegrams and telexes. They also provide for electronic signatures in bills of lading. They do not, however, define the term "document" which appears in a number of articles so some residual doubts must remain as to the extent to which full EDI processes are contemplated. There is room for further refinement and development of a common understanding as to what the interpretation of "document" is.

- **Convention on the Contract for the International Carriage of Goods by Road:** The Convention would require a protocol dealing solely with the problem of electronic transmission of commercial documents.

Business representatives on the Steering Group also made the observation that even where there are no institutional regulations prohibiting acceptance of electronic documents, some government offices tend to refuse them for various reasons, including the lack of proper facilities.

Observations

Form requirements are still found in many aspects of commercial activities, including those areas covered by the survey. Remaining form requirements are apparent and pose challenges for governments to tackle.

In the area of government services, as will be discussed in detail in the following section on "delivery of government services", there are likely to be requirements for electronic means to be used in order for governments to accept them, and there may be a need to closely follow progress in this area.

In the area of electronic contracting, we observed a relatively smaller number of exceptions that would prohibit usage of electronic means in contracts. Specific exceptions were observed in contracts for certain kinds of transactions, such as real estate purchases, wills, adoption and divorce. However, they seemed to pose no serious problems for the promotion of electronic commerce.

In the area of financial services, there remain mandatory form requirements in certain transactions, *e.g.* written disclosures, handwritten signatures on bills and checks and written forms for consumer credit. Certain transactions involving governments will be allowed to use electronic means, as governments gradually introduce systems for accepting them. Some of the others remain because of the necessity, for example, of protecting consumers, and it may require time before consumers become confident and trust them.

In the area of transportation and delivery services, form requirements in many cases were identified as originating from certain key international laws. Although the OECD may not be directly involved with the formation of these international laws, it may be necessary to encourage that they include clauses explicitly accepting electronic documents specified within.

5. Apply authentication technologies to delivery of government services

Declaration: "proceed with the application of electronic authentication technologies to enhance the delivery of government services and programmes to the public"

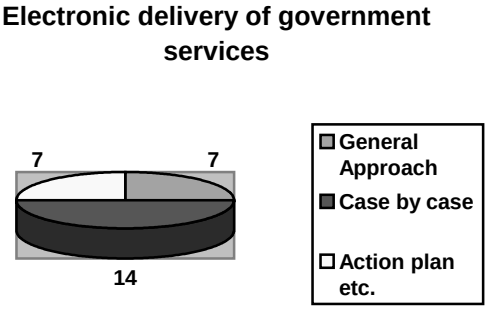
Findings

In the area of government services, initiatives coupled with legislation on electronic signatures have started. All of the 28 countries that have responded to the survey reported the existence of some kind of plan, work or actual implementation in this area. Typically, some countries started with tax or VAT services via electronic means, either as a pilot project or actual implementation of legislation that enabled electronic transactions.

There were case-by-case approaches and general approaches in grappling with existing laws, where the case-by-case approach would examine existing laws in a specific sector individually and amend them one by one whenever possible. The general approach typically involved a law containing an umbrella clause that would give legal recognition to electronic transactions, even when specific laws require certain form requirements. Of the 28 countries that responded, seven said that they have taken this general approach, and 14 reported the existence of pilot projects, or some projects in pioneering areas. Seven reported the existence of action plans, studies or works in this area, but supplied no information as to specific areas involved.

Observations

Developments in the area of government services are encouraging, in that almost all member governments



either have started initiatives to introduce electronic measures to be used in government services, or have plans to do so. It is not surprising that countries that are still planning or working on the electronic delivery of government services tend to be those that are still preparing specific laws on electronic signatures. Naturally, governments would first consider legislation to give legal recognition to electronic signatures and then use electronic signatures in their own services.

Although we observed divergences in approaches, namely between general and case-by-case approaches, the differences should not be overly emphasised at this stage. As long as governments share the common goal of achieving the delivery of government services through electronic means, the process of achieving that goal can differ depending on the countries' legal systems. The case-by-case approach is interpreted as an attempt to realise electronic delivery starting in the areas where such service is possible, effective, reasonable or easy. Typically, tax declarations or VAT systems fall under this category because, in their nature, they tend to have already been processed electronically, even before governments enabled electronic transactions as a matter of policy.

Since details of the systems in this area are still in the process of development, it is not possible to have concrete information as to the requirements electronic signatures must meet for transactions with governments. Even though party autonomy is ensured in commercial contracts, transactions with governments would most likely require the use of "secure" electronic signatures or other specific signatures that governments specify in their legal systems. Some governments explicitly reported their intention to accept only "secure" electronic signatures in their transactions. This may not cause specific problems concerning the objective of promoting electronic services in their systems, but it may justify further efforts to establish the interoperability of electronic authentication internationally.

Governments should be aware that even though laws might not explicitly reject the acceptance of electronic documents, the lack of proper facilities, equipment, infrastructures, or budget support might hinder the usage of electronic means.

6. Continue work at international level

Declaration: continue work at the international level, together with business, industry and user representatives, concerning authentication technologies and mechanisms to facilitate global electronic commerce

Findings

Joint OECD-Private Sector Workshop on Electronic Authentication

This joint OECD-Private Sector Workshop on Electronic Authentication was held on 2-4 June 1999 in Stanford and Menlo Park, California.

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

More than 200 participants attended the workshop. They included national delegations of member countries, members of the APEC Telecommunications Working Group, private sector representatives, consumer and user representatives, NGOs, representatives of international organisations and the OECD Secretariat and experts.

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

The Inventory on Authentication and Certification in a Global Networked Society [DSTI/ICCP/REG(2000)1/FINAL]

As OECD member 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 globally 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 an ongoing information exchange in order to clarify the issues related to authentication and certification and by providing a solid basis for ongoing international co-operation in this area. The WPISP continues the dialogue involving governments, business and industry, and user representatives to examine more fully the technologies and diverse models for

authentication and certification and to facilitate global electronic commerce, which is currently taking place or emerging in member countries.

The Inventory of Approaches to Authentication and Certification in a Global Networked Society was first published in October 1999 as DSTI/ICCP/REG(99)13/FINAL by the WPISP based on input supplied by member countries. The Inventory 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.

Since the first publication of the Inventory, rapid developments and policy changes including legislation that reflected the 1996 UNCITRAL (United Nations Commission on International Trade Law) Model Law, 1999 EU Directive for electronic signatures, and the 1998 OECD Ottawa Ministerial Declaration on Authentication for Electronic Commerce were observed among member governments.

The WPISP, at its 8th meeting on 4-5 May 2000, recognised the need to revise the Inventory with up-to-date information reflecting such policy developments in member governments, in the context of preparing a report on the implementation of the Ottawa Declaration on Authentication.

Although the information contained in the revised Inventory is up-dated as far as possible, 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 2000. The revised Inventory was reported to the WPISP at its meeting on 20-21 February 2001.

Observations

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 in the European Union and at the international level. The inventory should be considered a "work-in-progress" report that represents the ongoing information exchange among the members of the Working 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 member countries.

The revised 2000 Inventory illustrated, especially when compared with the previous Inventory, the somewhat remarkable developments and policy changes in member countries in the area of authentication and electronic signatures. There is no reason to assume these changes have lost their momentum at this stage. The information contained in the Inventory has some value in itself and, if the delegates so wish, we may continue gathering information and present it in the future as revised Inventories.

Conclusion

The Declaration on Authentication for Electronic Commerce — adopted by Ministers at the Ottawa Ministerial Conference on 7-9 October 1998 — recognised the importance of authentication for electronic commerce. It outlined a number of actions to promote the development and use of electronic authentication technologies and mechanisms, including continuing work at the international level, together with business, industry and user representatives.

With an approval of the ICCP, the WPISP decided to form a Steering Group to prepare a report on progress in the implementation of the Ottawa Declaration including initiatives developed and results achieved in member countries.

The Steering Group was established, and examined how national policies and laws are currently implemented with regard to facilitating legal recognition, party autonomy, technology neutrality, global authentication mechanisms and user confidence and ensuring that there is no legal discrimination in relation to different types of authentication technology. To this end the Steering Group has revised *the Inventory on Authentication and Certification in a Global Networked Society [DSTI/ICCP/REG(99)13/FINAL]* and has conducted a survey on form requirements, which have been identified as potentially major obstacles to the implementation of electronic authentication and electronic commerce.

In conducting the survey on form requirements, a questionnaire was developed under the auspices of Steering Group members, and then circulated among member governments *(Annex 2).*

In addition, the Steering Group continually collected information on the activities of APEC economies in this area through member delegates acting as liaisons to APEC.

The study was conducted for each item of the issues that the Declaration addressed.

- Legal recognition of electronic signatures.
- Favourable consideration to the UNCITRAL Model Law.
- Non-discriminatory approach to foreign authentication.
- Encouraging efforts to develop and facilitate the use of authentication technologies.
- Applying authentication technologies to the delivery of government services.
- Continuing work at the international level.

As for **the legal recognition of electronic signatures**, the progress after the October 1998 Ottawa Declaration is evident. In total, 17 member countries, not only EU member states, have amended technology or media-specific requirements in current laws or policies, where appropriate, and have given legal recognition to electronic signatures. Most of the other member countries either have drafts of amendments ready or work is underway. We might encourage continuing efforts in those countries that are preparing for legislation. We also might consider providing outreach with regard to these activities to non-OECD member countries.

As for **giving favourable consideration to the UNCITRAL Model Law**, clauses of the UNCITRAL Model Laws such as “legal recognition,” “variation by agreement” and “court admissibility” are commonly reflected in national legislation or regulation where amendments were made. It might be necessary to encourage continuing efforts in those countries that are preparing for legislation, and we also might

consider providing outreach to OECD non-member countries to encourage further adoption of the Model Law.

As for a **non-discriminatory approach to foreign authentication**, governments either express policies for non-discrimination, or remain silent about nationality of authentication, which is interpreted as being non-discriminatory to foreign authentication. However, the differences in standards or schemes among countries cause certain concern for the interoperability of electronic signatures and cross-certification of CAs. There seems to be a need for compatibility of approaches and policies among OECD member governments and business initiatives for the purpose of establishing international real marketplace interoperability of electronic authentication systems. To this end, member governments may wish to consider how global, seamless authentication and certification mechanisms should be developed in this area. Options may include:

a) Developing a scheme to follow the APEC's example in identifying and mapping the certification authority and accreditation linkages that are necessary for organisations to securely interact and transact with each other electronically across jurisdictional boundaries. It is recognised that there are differences in some of the approaches being taken. This project is expected to facilitate a pulling together of the different approaches and provide for an analysis of how the variances might be adapted to meet the same objectives. This could lead to interoperable electronic authentication systems among member countries. Through the experiences of the June 1999 joint OECD-Private Sector Workshop on Electronic Authentication in Stanford, it is apparent that different business models have emerged. This mapping exercise will help to encourage and facilitate real marketplace interoperability by highlighting commonalties and, moreover, recognising where differences need to be addressed.

b) Collecting and exchanging more detailed and specific information on some crucial aspects affecting interoperability of electronic certificates and authentication that have been in identified in various previous studies. These may include (See the EESSI activities in a previous section for more details):

- Quality and functional standards for certification service providers.
- Quality and functional standards for signature creation and verification products.
- Interoperable standardisation requirements for electronic signatures.

This exercise will help to encourage and facilitate real marketplace interoperability by recognising where differences need to be addressed.

As for **encouraging efforts to develop and facilitate the use of authentication technologies,** form requirements are still found in many aspects of commercial activities, including those areas the survey covered. Remaining form requirements are apparent and pose challenges for governments to tackle.

- In the area of the electronic contracting, we observed a relatively smaller number of exceptions, but they seemed to pose no serious problems for the promotion of electronic commerce.
- In the area of financial services, mandatory form requirements still remain in certain transactions, *e.g.* written disclosures, handwritten signatures on bills and checks, and written forms for consumer credit. Certain transactions involving governments will allow the use of electronic means, as governments gradually introduce systems for accepting them. Some of the others may remain because of the necessity, for example, of protecting consumers, and it may take time before consumers will become confident and trust electronic means. We may encourage further effort in this area.

- In the area of transportation and delivery services, form requirements in many cases were identified as originating from certain key international laws. Although the OECD may not be directly involved with the formation of these laws, it may be necessary for the OECD to encourage that they include clauses to explicitly accept electronic documents specified within.
- In the area of government services, there will likely be requirements for electronic means in order for the governments to accept. There may be a need to closely follow progress here.

As for **applying authentication technologies to the delivery of government services,** developments in this area are encouraging, in that almost all the member governments either have started initiatives to introduce electronic measures to be used in government services, or have plans to do so. Naturally, governments would first consider legislation to give legal recognition to electronic signatures and then use electronic signatures in their own services. The difference in approaches, namely between the general approach and the case-by-case approach, should not be overly emphasised at this stage. As long as governments share the common goal of achieving the delivery of government services through electronic means, the process of achieving that goal can be different depending on the legal systems of the countries. Even though party autonomy is ensured in commercial contracts, transactions with governments would most likely require the use of "secure" electronic signatures or other specific signatures that governments would specify in their legal systems. Some governments explicitly reported their intention to accept only "secure" electronic signatures in transactions with the government. This may not cause specific problems with the objective of promoting electronic services in their systems, but may justify further efforts to establish the interoperability of electronic authentication internationally. Governments also should be aware that even though laws might not explicitly reject the acceptance of electronic documents, the lack of proper facilities, equipment, or other items might hinder usage of electronic means.

As for **continuing work at the international level**, it is important to note that in many member countries, legal systems promoting the usage of electronic means are still being developed. The inventory should be considered a "work-in-progress" report that represents the ongoing information exchange among the members of the Working Party. The revised 2000 Inventory illustrated, especially when compared with the previous Inventory, the remarkable recent developments and policy changes in member countries in the area of authentication and electronic signatures. There is no reason to assume these changes have lost their momentum at this stage. The information contained in the Inventory has value in itself, and we may continue gathering information to present as revised Inventories in the future.

ANNEX 1: DECLARATION ON AUTHENTICATION FOR ELECTRONIC COMMERCE

Made by OECD Ministers at the Conference
"A Borderless World: Realising the Potential of Global Electronic Commerce"
7-9 October 1998, Ottawa, Canada

The Governments of OECD Member countries:

CONSIDERING:

- the significant social and economic benefits offered by information and communication technologies and electronic commerce;
- the leading role of industry in developing information and communication technologies and electronic commerce;
- the need for government and industry to foster user confidence to facilitate the growth of global electronic commerce;
- the rapid development of authentication technologies and mechanisms, and their importance in the context of global information and communication technologies and electronic commerce; and
- the potential impact that diverse national solutions for electronic authentication could have on the development of global electronic commerce.

RECOGNISING:

- that work is underway at the international level to facilitate transborder electronic transactions and the use of authentication technologies and mechanisms to foster the growth of global electronic commerce;
- that transacting parties may select appropriate mechanisms which meet their needs for authentication in conducting electronic commerce, including particular authentication technologies, contractual arrangements and other means of validating electronic transactions, and that they can use judicial and other means of dispute resolution to prove the validity of those transactions;
- that governments can play a role in promoting electronic commerce as a user of information and communication technologies, products and services, including electronic authentication mechanisms;
- that technology or media specific rules for recording, storing or transmitting information (for example, certain paper-based requirements) could impede the development of electronic commerce and the use of electronic authentication mechanisms;

- that, where appropriate, market-driven, rather than government imposed, standards and codes of practice can provide a useful tool for developing user confidence in global electronic commerce; and

- the continuing dialogue within the OECD — involving governments, business and industry, and user representatives — to discuss the technologies and diverse models for authentication to facilitate global electronic commerce which are currently in use or emerging in Member countries, and in particular the ongoing work of the Organisation through its Information, Computer and Communications Policy (ICCP) Committee, to facilitate information exchange by compiling an inventory of approaches to authentication and certification and convening joint OECD-private sector workshops in the year ahead.

DECLARE THEIR DETERMINATION TO:

- take a non-discriminatory approach to electronic authentication from other countries;

- encourage efforts to develop authentication technologies and mechanisms, and facilitate the use of those technologies and mechanisms for electronic commerce;

- 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 Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996;

- proceed with the application of electronic authentication technologies to enhance the delivery of government services and programmes to the public; and

- continue work at the international level, together with business, industry and user representatives, concerning authentication technologies and mechanisms to facilitate global electronic commerce.

ANNEX 2: QUESTIONNAIRE FOR THE SURVEY ON FORM REQUIREMENTS[1]

Scope

In responding to the following questions, delegates are not only requested to report on the present situation but also on changes which have occurred since the Ottawa Declaration. Respondents should also feel free to comment on other form requirements related to authentication arising from external regulations, such as consumer protection, that might affect contracts.

General questions

Ministers in Ottawa declared their determination 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 Model Law on Election Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996". What steps has your country taken to fulfil this commitment?

Likewise, Ministers in Ottawa declared that OECD members should "take a non-discriminatory approach to electronic authentication from other countries". How has your country met this commitment?

Has your country enacted general statutes, regulations or other norms to give legal effect to electronic signatures, electronic documents or electronic authentication mechanisms? If yes, please provide information on that enactment.

Has your country specified any technical or non-technical[2] requirements for the recognition of electronic signatures, electronic documents or electronic authentication mechanisms from other countries? If yes, please provide information on those requirements.

Has your country undertaken any study (whether by government, legal experts, or private sector bodies) to identify form requirements in existing law that may impede electronic transactions. For example, have specific requirements for a hand-written signature, paper contract or other physical form been catalogued and documented? Is it available to the public? If such a study has been done, can you summarise its conclusions? If not, what is your estimate of transactions that require paper written documents or hand-written signatures?

Electronic contracting

Does your country have form requirements on contracts that depend on whether the transaction was completed by paper, ink, written documents, handwritten signatures, electronic signatures, electronic

1. "Form requirements" are types of requirements in law that information, including signatures, be presented in certain forms such as in writing or by using a paper document.

2. Non-technical requirements are those such as requirements for licensing, root authorities, cross certification, third parties or external notaries

documents or electronic authentication mechanisms? If yes, please describe briefly such requirements, including the nature (mandatory…)[3] and the origin (national law, regulation, and regional law…)[4] of the requirements.

Are there any statutes, regulations or other norms that provide for form requirements, of a technical or non technical nature, relating to the authentication or signature, in the matters of legal recognition, filing, recording or court admissibility of documents in electronic form. If yes, please describe briefly such requirements, including the nature (mandatory…)[5] and the origin (national law, regulation, and regional law…)[6] of the requirements.

If yes to Q7), please specify whether legal recognition will be provided to individual contracting parties that agree to use electronic documents.

Where one party from one country contracts with another party from a different country, are there any form requirements imposed on the party from the other country? Are there different form requirements imposed on the party from the other country or are they applied in a different manner? If so, what are they and what is the public policy underlying such form requirements?

Financial services

Does your country have form requirements on transactions in the following categories of financial services?

- Intra-company Financial services (Employee stock purchases, options, retirement accounts, and pension plans)
- B-2-B Commercial Banking
- B-2-B Commercial Lending
- B-2-B Investment Banking, Commercial financing
- B-2-C Consumer Banking
- B-2-C Consumer Lending
- B-2-C Brokerage, Stock Trading

If yes, please give reference information including the nature (mandatory…)[7] and the origin (national law, regulation, and regional law …)[8] of the requirements.

---

3. The nature of the requirement should be determined from the point of view of the **degree of the obligation**. Is it **mandatory**, **prerequisite**, **arbitrary** or does any **leeway** exist?

4. The origin of the form requirements shall give information whether they are resulting from a national law, regulation, regional law, international agreement, etc…

5. The nature of the requirement should be determined from the point of view of the **degree of the obligation**. Is it **mandatory**, **prerequisite**, **arbitrary** or does any **leeway** exist?

6. The origin of the form requirements shall give information whether they are resulting from a national law, regulation, regional law, international agreement, etc…

7. The nature of the requirement should be determined from the point of view of the **degree of the obligation**. Is it **mandatory**, **prerequisite**, **arbitrary** or does any **leeway** exist?

8. The origin of the form requirements shall give information whether they are resulting from a national law, regulation, regional law, international agreement, etc…

Are there any statutes, regulations or other norms that recognise the use of electronic signatures or electronic authentication mechanisms in the transactions listed in Q10)? If yes, are there any technical or non-technical[9] requirements specified? Please give reference information including information as to why such technical requirements are necessary.

If no to Q11), please give reference information including why electronic signatures or electronic authentication mechanisms are not accepted. Also, are there any statutes, regulation or other norms that allow parties to vary these requirements among themselves by agreement of the parties, or, are there any restrictions to the rights of parties to choose the proper forms or technology for a given transaction?

Does the usage of electronic signatures or electronic authentication mechanisms have the same legal consequences as paper written documents or hand written signatures under your country's form requirements in Q10)? If no, please give reference information as to how different legal consequences are under them and why?

Transportation and delivery services

Does your country have form requirements on transactions in the following categories of transportation transactions especially on the following documents: Bills of Lading, Waybill, Manifest to regulatory authority, declaration by importers, declaration by exporters, dangerous goods exports, invoice?

- Intra-company logistics
- B-2-B Commercial Trade
- B-2-C Delivery of Goods
- C-2-C Shipments

If yes, please give reference information including the nature (mandatory…)[10] and the origin (national law, regulation, and regional law…)[11] of the requirements.

Are there any statutes, regulations or other norms that recognise the use of electronic signature or electronic authentication mechanisms in the transactions listed in Q14)? If yes, are there any technical or non-technical[12] requirements specified? Please give reference information including information as to why such technical requirements are necessary.

If no to Q15), please give reference information including why electronic signatures or electronic authentication mechanisms are not accepted. Also, are there any statutes, regulations or other norms that allow parties to vary these requirements among themselves by agreement of the parties, or, are there any restrictions to the rights of parties to choose the proper forms or technology for a given transaction?

9. Non-technical requirements are those such as requirements for licensing, root authorities, cross certification, third parties or external notaries

10. The nature of the requirement should be determined from the point of view of the **degree of the obligation**. Is it **mandatory**, **prerequisite**, **arbitrary** or does any **leeway** exist?

11. The origin of the form requirements shall give information whether they are resulting from a national law, regulation, regional law, international agreement, etc…

12. Non-technical requirements are those such as requirements for licensing, root authorities, cross certification, third parties or external notaries.

Does the usage of electronic signatures or electronic authentication mechanisms have the same legal consequences as paper written documents or hand written signatures under your country's form requirements in Q14)? If no, please give reference information as to how different legal consequences are under them and why?

Government services

Ministers in Ottawa stated their determination to "proceed with the application of electronic authentication technologies to enhance the delivery of government services and programmes to the public". Please describe your country's efforts in this regard.

Does your country have a policy on the nature of authentication that may be used by citizens and businesses in on-line dealings with the Government? If yes, how is that policy delivered and to what extent does the policy allow authentication services originated in other countries to be used by your citizens and businesses? Also, to what extent has that policy been developed in conjunction with authentication service vendors and user representatives?

Does your country have form requirements on transactions in the following categories of government services?

- G-2-B Procurement/Sales
- G-2-B VAT
- G-2-B Tax
- B-2-C including benefit claims
- Other areas

If yes, please give reference information including the nature (mandatory…)[13] and the origin (national law, regulation, and regional law…)[14] of the requirements.

Are there any statutes, regulations or other norms that recognise the use of electronic signature and electronic authentication mechanisms in the transactions listed in Q20)? If yes, are there any technical or non-technical[15] requirements specified? Please give reference information including information as to why such technical requirements are necessary.

(If no to Q21), please give reference information including why electronic signatures or electronic authentication mechanisms are not accepted. Also, are there any statutes, regulations or other norms that allow parties to vary these requirements among themselves by agreement of the parties, or, are there any restrictions to the rights of parties to choose the proper forms or technology for a given transaction?

13. The nature of the requirement should be determined from the point of view of the **degree of the obligation**. Is it **mandatory**, **prerequisite**, **arbitrary** or does any **leeway** exist?

14. The origin of the form requirements shall give information whether they are resulting from a national law, regulation, regional law, international agreement, etc.

15. Non-technical requirements are those such as requirements for licensing, root authorities, cross certification, third parties or external notaries.

ANNEX 3: TABLE ON HOW MEMBER COUNTRIES IMPLEMENTED THE OTTAWA DECLARATION

Member countries	Have steps been taken for the 1996 UNCITRAL Model Law on E-Commerce?	Specific law? A specific national law or regulation concerning digital or electronic signatures?	When will/did it become effective?	Notion of secure signature?
Australia	Yes	Yes	March 2000	General legal requirements
Austria	Yes	Yes	Jan 2000	EU Directive
Belgium	Yes	Yes, now before the Parliament	Now before the Parliament	EU Directive
Canada	Yes	Yes	May 2000	Secure ES with Govt
Czech Republic	Yes	Yes	Oct 2000	Compliance with EU Directive
Denmark	Yes	Yes	Oct 2000	EU Directive
Finland	Yes	Drafting	Drafting(Jan 2000 for govt)	EU Directive
France	Yes	Yes	March 2000	EU Directive
Germany	Yes, in preparation	Yes	Aug 1997	EU Directive
Greece	No, but already in compliance	No, but related laws give evidential value	1997 (EU Directive in progress)	EU Directive (in progress)
Hungary	Yes	Yes	Jan 2001	Compliance with EU Directive
Iceland	No	No, Work underway	-	-
Ireland	Yes in preparation of legislation	Not yet	-	EU Directive
Italy	Yes	Yes	March 1997	EU Directive
Japan	Yes	Yes	April 2001	Voluntary accredited CA
Korea	Yes	Yes	Feb 1999	Digital signature
Mexico	Yes preparing for modification	No, but parties are free to agree	Review of Commercial Law in progress	-
Netherlands	Yes	Yes, by July 2001	Aimed July 2001	EU Directive
New Zealand	Yes	Yes now drafted	2001?	-
Norway	Yes	Yes by July 2001	July 2001	Compliance with EU Directive
Poland	Yes	Being prepared	-	-
Portugal	Yes	Yes	Aug 1999	EU Directive
Spain	Yes	Yes	Oct 1999	EU Directive
Sweden	Yes	Yes	Jan 2001	EU Directive (qualified signature)
Switzerland	Yes	Yes by notice of Office of Justice	Nov 1998	Secure PKI “Swisskey”
Turkey	No	No	Work is underway	-
United Kingdom	Yes	Yes	May 2000	Digital certificates “tScheme”
United States	Yes	Yes (UETA and states)	1999(UETA), 2000(E-SIGN)	No

	Recognise foreign electronic signatures?	Scheme for accrediting CA?	Government Service use electronic signatures?
Australia	Yes	Yes	All by the end of 2001
Austria	Law in preparation	In preparation	Court, social security, healthcare, some financial data
Belgium	Law in preparation	Yes	All by the end of 2001
Canada	Yes	Yes	Federal Act permits use of secure ES with Govt
Czech Republic	Yes	In preparation	Action plan exists
Denmark	Yes	Yes	Several public authorities have implemented services
Finland	Yes	No	More than 100 pilot schemes
France	Yes	Yes	VAT, Tax, health, custom etc.
Germany	Yes	Yes	A large number of pilot projects with future basket law
Greece	No	In preparation	Experiments on VAT
Hungary	Yes	Yes in preparation	All public procurement by the end of 2001
Iceland	-	-	Work underway
Ireland	Will be yes	-	Work underway
Italy	Yes	Yes	Procurement, tax, real estate lease, etc.
Japan	Yes	Yes	By 2003
Korea	Yes by mutual agreement	Yes	Plan to amend laws
Mexico	Yes	Yes	Payment system, taxation, public register etc.
Netherlands	No	Yes	Many pilot projects. 25% in 2002
New Zealand	No	Yes	Income tax returns
Norway	Yes	Yes	Pilot project on Tax returns
Poland	No	Yes	Planning
Portugal	-	In planning	Planning
Spain	-	In preparation	Tax
Sweden	Yes	Yes	Various pilot projects
Switzerland	-	Yes	Tax
Turkey	No	No	Custom, pilot projects in exports
United Kingdom	Yes	Yes	All by 2005
United States	Yes	Yes	All

ANNEX 4: SUMMARY TABLE: SURVEY ON FORM REQUIREMENTS / GENERAL QUESTIONS

Questions	Australia	Austria	Belgium
1) What amendments have been made in order to improve the use of information and communication technologies and electronic authentication mechanisms?	The Commonwealth Electronic Transactions Act came into operation on March 2000. The Act follows the UNCITRAL Model Law. Australia will have national uniform electronic transactions laws in place by the end of 2000.	Austria already implemented the EU-Directive on a common framework for electronic signatures in the Austrian Electronic Signature Act.	Electronic signatures will be legally accepted and considered as equivalent to the manuscript signature in the near future, following the approval on 6 October 2000 by the Belgian Federal Council of Ministers of a draft Law concerning the activities of certification service providers for the use of electronic signatures.
2) What has been done in order to take a non-discriminatory approach to electronic authentication from other countries?	The act is technology neutral and non-discriminatory to foreign technologies as long as it satisfies the minimum standards of the act.	According to the EU-Directive, certificates issued by foreign certification service providers shall be tantamount to Austrian certificates, if necessary, under a bilateral or multilateral agreement between the European Community on the one hand and third countries or international organisations on the other hand.	The EU-Directive 1999/93/EC imposes a non-discriminatory approach within the European Community and, in some cases (see article 7), toward those foreign certification service providers issuing qualified certificates.
3) Any general statutes, regulations or other norms that give legal effect to electronic signatures?	Yes	Yes	Not yet.
3)a) If yes to Q3), please provide information on that enactment.	Electronic Transactions Act 2000; Uniform Electronic Transactions Bill	Electronic Signature Act	A draft Law to amend the Civil Code provisions about evidence is currently before the Parliament.
4) Any requirements for foreign authentication?	No	Yes	Not yet.
4)a) If yes to Q4), provide information on those requirements.	#	A security confirmation of a confirmation body according to the EU-Directive on electronic signatures is required, which has the task to determine the conformity of secure signature creation devices with the requirements laid down in the EU-Directive.	After implementation of the EU-Directive, some requirements for “qualified signatures” (see article 7).
5) Any study that identified form requirements in existing law?	Yes	Yes	No
5)a) Have specific requirements for a hand-written or paper documents been catalogued and documented?	?	The study identified the form requirements in existing law prior to the Electronic Signature Act.	#
5)b) Is this documentation available to the public?	Yes	?	#
5)c) If yes to Q5), can you summarise its conclusions?	The number of legal form requirements that will not be able to be satisfied by the use of electronic communications should be extremely limited and easily identifiable in the Act.	In Austria exist only few legal form requirements for the valid conclusion of a contract.	#
5)d) If no to Q5), what is your estimate of transactions that require paper written documents or hand-written signatures?	#	#	?

Note: BIAC inputs are added as **bold with underlines**

Questions	Canada	Czech Republic	Finland
1) What amendments have been made in order to improve the use of information and communication technologies and electronic authentication mechanisms?	On April 13 2000, the federal Personal Information Protection and Electronic Documents Act was passed. The provisions for electronic signatures came into effect in May 2000, and for protection of personal information in January 2001. However, contracts are regulated provincially, and one province has enacted legislation and four others have proposed.	No Electronic Signature Act has yet been included into the Czech legislation. A draft Electronic Signature Act will enter into force once it has been published. The bill is in accordance with the EU Directive 1999/93/EC.	The implementation of the EU Directive for electronic signatures is under drafting in Finland. In the private sector, Finnish legal system allows the use of digital or electronic signatures without restriction. However, Finland underlines the importance of non-regulation. In the public sector, the Act on electronic transactions with public authorities has been valid since Jan. 2000.
2) What has been done in order to take a non-discriminatory approach to electronic authentication from other countries?	The federal Personal Information Protection and Electronic Documents Act does not discriminate against electronic authentication from other countries. Provincial legislations are silent about this.	The bill also treats about the issue of acknowledgement of foreign qualified certificates.	Finland is non-discriminatory to the electronic authentication from other countries.
3) Any general statutes, regulations or other norms that give legal effect to electronic signatures?	Yes	Under consideration	Yes
3)a) If yes to Q3), please provide information on that enactment.	The federal Personal Information Protection and Electronic Document Act will provide for the use of “secure electronic signature” under general requirements	Draft Electronic Signature Act	Act on Electronic Service in the Administration
4) Any requirements for foreign authentication?	No	?	Yes
4)a) If yes to Q4), provide information on those requirements.	#	?	The mentioned act will contain some technical and non-technical requirements which will apply as well to recognition of electronic signatures, electronic documents and authentication mechanisms from other countries.
5) Any study that identified form requirements in existing law?	Yes	?	Studies in this area have been undertaken, but there was no attempt to catalogue all form requirements in existing law.
5)a) Have specific requirements for a hand-written or paper documents been catalogued and documented?	In May 1998, “Consultation Paper, Facilitating Electronic Commerce: Statues, Signatures and Evidence” was released.	?	There was no attempt to catalogue all form requirements that can not be fulfilled electronically.
5)b) Is this documentation available to the public?	Yes http://canada.justice.gc.ca/cn/dept/index.html	?	Yes
5)c) If yes to Q5), can you summarise its conclusions?	Of the nearly 600 federal public statues, the Paper states that 330 statues contain language that uses words like “form”, “application”, “signature”, “records,” etc.	?	It is important that no unnecessary barriers to modern transaction methods are raised by legislation. If an electronic signature is deemed not to meet the formal requirements for transactions where electronic data exchange is to be used, the easing of those requirements should be considered, case by case.
5)d) If no to Q5), what is your estimate of transactions that require paper written documents or hand-written signatures?	#	?	?

Questions	France	Germany	Italy
1) What amendments have been made in order to improve the use of information and communication technologies and electronic authentication mechanisms?	Transposition of the EU directive in progress in three stages: 1) Law of 13 March 2000 giving equivalence under conditions between ES and handwritten signature 2) Decree of Council of State at the end of 2000 on the requirements for allowing a presumption of reliability for ES. 3) The responsibility for the providers of electronic certification will be addressed in the future law for the Information Society, to be published at the beginning of 2001		In 1997 Italy issued a Presidential Decree (No. 513), giving juridical value to the electronic document. The same decree establishes the full equality between hand-written signature and digital signature. Such topic has been fully regulated by a following specific technical regulation.
2) What has been done in order to take a non-discriminatory approach to electronic authentication from other countries?	Non-discriminatory, as in the European directive	According to the EU-Directive, certificates issued by foreign certification service providers are recognised, if necessary, under a bilateral or multilateral agreement between the European Community on the one hand and third countries or international organisations on the other hand.	There is an ongoing reception of the European Directive (1999/93/CE). The Presidential Decree No. 513/1997, section 8.4, already recognises the value of digital certificates issued by Certification Authorities (CAs) of other European countries.; **it doesn't specify any different treatment for extra-EU parties.**
3) Any general statutes, regulations or other norms that give legal effect to electronic signatures?	Yes - under consideration	Yes	Yes
3)a) If yes to Q3), please provide information on that enactment.	In the Decree of the Q1	Draft Law Civil Code 06.09.2000: http://www.sicherheit-im-Internet.de/download/BGB-AenderungReferentenentwurf9-2000.pdf; Draft Project Public law not yet published.	The related set of rules are: Law No. 59/1997, section 15.2; Presidential Decree No. 513/1997; Prime Minister Decree of 8 February 1999; Circular No. 22 of 26 July 1999 issued by the Authority for IT in the Public Administration (AIPA); Presidential Decree No. 498 of 20 October 1998; AIPA Deliberation No. 24/1998; Presidential Decree No. 70 of March 1999; AIPA Circular No. 24/2000
4) Any requirements for foreign authentication?	Yes - under consideration	Yes	Yes
4)a) If yes to Q4), provide information on those requirements.	Principles of the EU Directive	A security confirmation of a confirmation body according to the EU-Directive on electronic signatures is required, which has the task to determine the conformity of secure signature creation devices with the requirements laid down in the EU-Directive.	Lawful value only to digital signatures that respect the above set of norms. The Presidential Decree No. 513/1997 gives full validity to the digital certificates issued by CAs of EU Member States if they are compliant with the requirements of the decree.
5) Any study that identified form requirements in existing law?	No	No: for Private Law area. — Yes: for Public Law area	In the Italian legal system there are not legal rules prohibiting electronic transactions.
5)a) Have specific requirements for a hand-written or paper documents been catalogued and documented?	No	a) See Draft Law Civil Code; b) Public Law: The Federal Ministry of Interior did a survey which is not published.	Some acts must be in written form: hand-written testaments, penal sentences, shares, etc.
5)b) Is this available to the public?	-	a) Yes b) No	#
5)c) If yes to Q5), can you summarise its conclusions?	-	In Germany exist only few legal form requirements for the valid conclusion of a contract.	Some acts must be in written form: hand-written testaments, penal sentences, shares, etc.
5)d) If no to Q5), what is your estimate of transactions that require paper written documents or hand-written signatures?	?	#	#

Questions	Japan	Korea	Netherlands
1) What amendments have been made in order to improve the use of information and communication technologies and electronic authentication mechanisms?	Japanese Law Concerning Electronic Signatures and Certification Services will be enforced from April 1, 2001.	Korea enacted the Digital Signature Act and the Basic Law on Electronic Commerce in February 1999.	The Netherlands does not have yet a specific law concerning electronic signatures, but one is currently drafted to implement the EU-directive on electronic signatures in national legislation. The aim is to have this legislation in place July 2001.
2) What has been done in order to take a non-discriminatory approach to electronic authentication from other countries?	By mutual governmental approval, the certifications from a foreign country can have the same legal effect and status as Japanese certifications.	By mutual governmental approval, the certifications from a foreign country can have the same legal effect and status as South Korean certifications.	The principle of free evidence reflects in fact the non-discriminatory approach.
3) Any general statutes, regulations or other norms that give legal effect to electronic signatures?	Under consideration	Yes	No. However, the principle of free evidence under current law already allows electronic signatures for evidentiary purposes.
3)a) If yes to Q3), please provide information on that enactment.	Japanese Law Concerning Electronic Signatures and Certification Services.	Digital Signature Act; Basic Law on Electronic Commerce	#
4) Any requirements for foreign authentication?	?	No	No
4)a) If yes to Q4), provide information on those requirements.	?	#	#
5) Any study that identified form requirements in existing law?	No	Studies are under way.	?
5)a) Have specific requirements for a hand-written or paper documents been catalogued and documented?	No	?	?
5)b) Is this documentation available to the public?	#	?	?
5)c) If yes to Q5), can you summarise its conclusions?	#	?	?
5)d) If no to Q5), what is your estimate of transactions that require paper written documents or hand-written signatures?	?	?	?

Questions	Norway	Portugal	Sweden
1) What amendments have been made in order to improve the use of information and communication technologies and electronic authentication mechanisms?	Norway is in the process of implementing the EU Directive 1999/93/EC on Electronic Signature in a new Act on Electronic Signature. The act, together with secondary legislation, will enter into force in July 2001. Simultaneously, Norway has drafted a "formal statement" establishing that in general a document can be drafted and signed electronically.	The Decree-Law nº 290-D/99 and the Council of Ministers Resolution nº 115/98 decided that the definition of the legal framework applicable to electronic documents and digital signatures is one of the objectives to be achieved.	In the private sector there are very few legal impediments. In the public sector the Swedish Government recently presented an IT bill with the intention to let the public sector become a pioneer in the use of IT in society. There is a proposal for new Act on Qualified Electronic Signatures.
2) What has been done in order to take a non-discriminatory approach to electronic authentication from other countries?	The EU Directive contains non-discriminatory regulations in relation to those foreign certification service providers issuing "qualified certificates."	?	The Swedish legal system does not take a discriminatory approach to electronic authentication from other countries.
3) Any general statutes, regulations or other norms that give legal effect to electronic signatures?	With regard to the characteristics of the Norwegian legal system and given the principle of free evidence, this is considered not necessary.	No	No. But it should, however, be noted that electronic signatures, electronic documents and electronic authentication mechanisms are already admissible in Sweden.
3)a) If yes to Q3), please provide information on that enactment.	#	#	
4) Any requirements for foreign authentication?	No	?	No
4)a) If yes to Q4), provide information on those requirements.	#	?	#
5) Any study that identified form requirements in existing law?	Yes	No	Yes
5)a) Have specific requirements for a hand-written or paper documents been catalogued and documented?	Norway is undertaking a large survey to find all legal impediments for electronic signatures.	?	In 1996, a minor survey of form requirements was undertaken.
5)b) Is this available to the public?	Yes	?	Yes
5)c) If yes to Q5), can you summarise its conclusions?	1) It is not possible to draft one general act that put electronic communication on par with paper-based communication. 2) The approach used in this project is akin to the UNCITRAL functional equivalent approach.	?	Electronic means are not excluded. There are however other form requirements that can impede use of electronic communication. Changes will have to be made in the relevant act or regulation if electronic means for authentication shall be accepted. Form requirements of this nature where found primarily in regulations which are inferior to acts. **(*)**
5)d) If no to Q5), what is your estimate of transactions that require paper written documents or hand-written signatures?	#	Today it is possible to ensure the trustworthiness and integrity of electronic documents, using means assuring a much higher quality than the existing means for paper mediums.	**(*)There are a number of form requirements. Most of them concern the public administration. There are few requirements in civil law. It has been argued that a single act on form requirements is not practicable**.

Note: BIAC inputs are added as **bold with underlines**

Questions	Switzerland	Turkey	United Kingdom
1) What amendments have been made in order to improve the use of information and communication technologies and electronic authentication mechanisms?	The Ordinance on Electronic Certification Services (OSCert), was enforced in May 2000. It is experimental and will be replaced by a law on electronic signatures which is in course of elaboration.	Electronic signatures and electronic authentication mechanisms have not been given legal effect in Turkey yet.	The Electronic Communications Act 2000, which passed into law on 25 May, gives UK Ministers the power to amend existing legislation, where appropriate, to enable electronic communications to be accepted in areas where the law currently specifies traditional methods.
2) What has been done in order to take a non – discriminatory approach to electronic authentication from other countries?	The mentioned ordinance follow the principles of international agreements concerning the international recognition of electronic signature.	There are no different form requirements imposed on the party from another country nor are they applied in a different manner.	The Act does not make special provisions for electronic signatures of UK origin or for those originating elsewhere. Both are admissible and it is for the court to decide their validity and relevance in the context of a particular case.
3) Any general statutes, regulations or other norms that give legal effect to electronic signatures?	Under consideration	No	Yes
3)a) If yes to Q3), please provide information on that enactment.	The Ordinance on Electronic Signatures (OSCert) will be presented to parliament in 2001. There is no fixed calendar yet for the enactment.	#	Part II Section 7 of the Electronic Communications Act
4) Any requirements for foreign authentication?	Yes	No	No
4)a) If yes to Q4), provide information on those requirements.	The only requirement is to use reliable systems and computational products in function of the technical evolution.	#	#
5) Any study that identified form requirements in existing law?	Yes	No	Studies are under way.
5)a) Have specific requirements for a hand-written or paper documents been catalogued and documented?	There is a report about form requirements in Contract Law.	No	No
5)b) Is this documentation available to the public?	No	#	#
5)c) If yes to Q5), can you summarise its conclusions?	In Contract Law, electronic signatures can present problems in the domain of certain transactions and in all the cases where the signature aims to protect the consumer against premature decisions.	#	#
5)d) If no to Q5), what is your estimate of transactions that require paper written documents or hand-written signatures?	?	?	#

Note: BIAC inputs are added as **bold with underlines**

Questions	United States	EU
1) What amendments have been made in order to improve the use of information and communication technologies and electronic authentication mechanisms?	**The US recently passed a national electronic signature law along the lines of the UNCITRAL Model law**. In August, 2000, twenty-two (22) states have adopted the Uniform Electronic Transactions Act (UETA); the Federal "E-Sign" Law signed by the President in June 2000 becomes effective in October 2000; the Government Paperwork Elimination Act (GPEA) is in force since October 1998.	**The European Parliament and the Council approved on 13 December 1999 the Directive 1999/93/EC on a Community framework for electronic signature, largely inspired from the still on-going activities led by UNCITRAL. The Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this directive before 19 July 2001.**
2) What has been done in order to take a non –discriminatory approach to electronic authentication from other countries?	The UETA reflects the non-discriminatory approach to electronic authentication from other countries. Moreover, the US has signed numerous Joint Statements on Electronic Commerce that include commitments to non-discrimination.	**The Directive explicitly states that "in order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services".**
3) Any general statutes, regulations or other norms that give legal effect to electronic signatures?	Yes	
3)a) If yes to Q3), please provide information on that enactment.	Uniform Electronic Transaction Act (UETA) in at least 22 states; Federal "E-Sign" Law; Government Paperwork Elimination Act (GPEA) .**There are a few state laws which provide a presumption to persons/entities using specified signature technologies, but it is unclear if those state acts are in conformance with the new national law.**	**The Directive states that "advanced electronic signatures satisfy the legal requirements of a signature in relation to data in electronic form and are admissible as evidence in legal proceedings. An electronic signature is not denied legal effectiveness and admissibility solely on the ground that it is in electronic form, or not based on a qualified certificate etc..**
4) Any requirements for foreign authentication?	No	
4)a) If yes to Q4), provide information on those requirements.	# **No, with the exception of the minority of States mentioned above.**	**The European Electronic Signature Standardisation Initiative (EESSI), an industry-led initiative, proposed a set of industry standards to facilitate cross border recognition. EESSI will interface with the "Electronic Signature Committee", appointed by the Directive.**
5) Any study that identified form requirements in existing law?	Yes	**Several studies have been led in the different Member States of the EU on form requirements.**
5)a) Have specific requirements for a hand-written or paper documents been catalogued and documented?	A report addresses the "bottom line" concern that some existing form requirements may still need to exist to ensure certain public policy objectives.	
5)b) Is this documentation available to the public?	Yes	**There is presently at our knowledge no synthesis available.**
5)c) If yes to Q5), can you summarise its conclusions?	?	**For commercial operations, the Directive states that "the freedom of parties to agree between themselves .... should be respected ...; the legal effectiveness of electronic signatures...and their admissibility ...should be recognised". For administrative rules an important effort is presently done in most Member States to achieve on-line procedures.**
5)d) If no to Q5), what is your estimate of transactions that require paper written documents or hand-written signatures?	E-SIGN also contains consumer safeguards provisions that require all critical notices to be sent on paper.	

Note: BIAC inputs are added as **bold with underlines**

Questions	**BIAC**
1) What amendments have been made in order to improve the use of information and communication technologies and electronic authentication mechanisms?	*The BIAC response provides information on: CANADA, EU, ITALY, SWEDEN, US.*
2) What has been done in order to take a non – discriminatory approach to electronic authentication from other countries?	*The BIAC response provides information on: CANADA, EU, ITALY, SWEDEN, US.*
3) Any general statutes, regulations or other norms that give legal effect to electronic signatures?	*The BIAC response provides information on: CANADA, EU, GERMANY, ITALY, SWEDEN, US.*
3)a) If yes to Q3), please provide information on that enactment.	See above.
4) Any requirements for foreign authentication?	*The BIAC response provides information on: CANADA, EU, ITALY, SWEDEN, US.*
4)a) If yes to Q4), provide information on those requirements.	See above.
5) Any study that identified form requirements in existing law?	The BIAC response provides information on: CANADA, EU, ITALY, SWEDEN.
5)a) Have specific requirements for a hand-written or paper documents been catalogued and documented?	See above.
5)b) Is this documentation available to the public?	See above.
5)c) If yes to Q5), can you summarise its conclusions?	See above.
5)d) If no to Q5), what is your estimate of transactions that require paper written documents or hand-written signatures?	See above.

Note: BIAC inputs are added as **bold with underlines**

ANNEX 5: SUMMARY TABLE: SURVEY ON FORM REQUIREMENTS / ELECTRONIC CONTRACTING

Questions	Australia	Austria	Belgium
6) Does your country have form requirements on contracts that depend on whether the transaction was completed by paper, hand written signatures, or electronic signatures?	No, but written evidence of a contract may be required in some circumstances through the operation of legislation.	Austrian Civil Code: Principally the form of contract is unrestricted, but handwritten signature is necessary when a legal provision requires the form of writing.	No, but written evidence of a contract may be required in some circumstances through the operation of legislation (e.g. a Law concerning consumers protection or an article of the Civil Code which imposes a written declaration for recognising debts).
6b) Nature of such requirements?	?	?	#
6b) Origin of such requirements?	?	?	#
7) Are there any statutes, regulations providing for form requirements in legal proceedings, of a technical or non-technical nature?	No. But in some instances the rules of courts and tribunals may contain form requirements that may limit the use of electronic communications.	No	See Q6
7a) Nature of such regulations?	?	#	#
7)b) Origin of such regulations?	?	#	#
8) If yes to Q7), will legal recognition be provided to individual contracting parties that agree to use electronic documents?	Where contracting parties agree to use electronic communications (or documents) in a transaction the transaction will not be invalid merely because the parties used electronic communications.	#	#
9) Are there any form requirements imposed on the party from the other country?	No	No, but in the case of cross border transactions you have to respect the rules of the private international law (Rome Convention on contractual obligations).	No, but in the case of cross border transactions, rules of the Private International Law (Rome Convention on contractual obligations) have to be respected.
9a) Are there different form requirements imposed on the party from the other country or are they applied in a different manner?	No	No	No
9b) What are they and what is the public policy underlying such form requirements?	#	#	#

Note: BIAC inputs are added as **bold with underlines**

Questions	Canada	Finland	Germany
6) Does your country have form requirements on contracts that depend on whether the transaction was completed by paper, hand written signatures, or electronic signatures?	Most provinces statutes require particular contracts to be reduced to writing (e.g. provincial Statute of Frauds, Consumer Protection Act, and Sale of Goods Act). Where statutes require certain contracts to be reduced to writing, those provisions are mandatory in nature.	No, except for few exceptions.	German Civil Code: Principally the form of contract is unrestricted, but handwritten signature is necessary when a legal provision requires, (many exceptions (hundreds)) the form of writing (such as real estate transactions). The general rule is: No form requirements for civil law contracts. Oral agreement is possible irrespective of the value. "Writing" means: document with hand-written signature
6b) Nature of such requirements?	mandatory	?	The Contract is not valid if requirements are not met.
6b) Origin of such requirements?	regional law	?	
7) Are there any statutes, regulations providing for form requirements in legal proceedings, of a technical or non-technical nature?	The federal Personal Information Protection and Electronic Documents Act state that the "best evidence rule" for any electronic document will be satisfied under certain conditions. The evidentiary presumptions will relate to documents signed with secure electronic signatures and will be established by regulation, as yet unwritten.	?	No
7a) Nature of such regulations?	Applies only to criminal proceedings and proceedings brought in the Federal Court of Canada.	?	#
7)b) Origin of such regulations?	Federal law	?	#
8) If yes to Q7), will legal recognition be provided to individual contracting parties that agree to use electronic documents?	Electronic commerce legislation enacted by one province and proposed in four other provinces acknowledges that contracts may be formed by electronic means.	The principle of freedom of contract applies always between two contracting parties and therefore all contracts that are made electronically, can be accepted in the court of law except for some specific contract types	#
9) Are there any form requirements imposed on the party from the other country?	No Canada does not impose any statutory form requirements on a party from a different country who or which contracts with a Canadian party	No	No, but in the case of cross border transactions you have to respect the rules of the private international law (Rome Convention on contractual obligations).
9a) Are there different form requirements imposed on the party from the other country or are they applied in a different manner?	No	No	No If German law is the basis of a transborder contract, German form requirements are binding. If the law of other countries rules the contract, their regulations are binding.
9b) What are they and what is the public policy underlying such form requirements?	#	#	#

Note: BIAC inputs are added as **bold with underlines**

Questions	Italy	Korea	Netherlands
6) Does your country have form requirements on contracts that depend on whether the transaction was completed by paper, hand written signatures, or electronic signatures?	There are not specific form requirements for contracts. However in particular cases the written form is required: ad substantiam, when it constitutes an essential element of the contract .- ad probationem, with the only aim of proof. **The electronic signatures, electronic documents or electronic authentication mechanisms are subject to the form requirements specified in the DPR 513/97; if the requirements are not met the document is not legally recognised.**	No	No
6b) Nature of such requirements?	For ad substantiam, The contract is not valid if this form requirement is not respected	#	#
6b) Origin of such requirements?	?	#	#
7) Are there any statutes, regulations providing for form requirements in legal proceedings, of a technical or non-technical nature?	The Prime Minister Decree of 8 February 1999 giving "Technical rules for creation, transfer, storage, duplication, reproduction and validation, of electronic documents."	No	No
7a) Nature of such regulations?	#	#	#
7)b) Origin of such regulations?	National Decree	#	#
8) If yes to Q7), will legal recognition be provided to individual contracting parties that agree to use electronic documents?	There are not specific form requirements for contracts. However in particular cases the written form is required: **legal recognition is assured to individual contracting parties that agree to use electronic documents also.**	#	#
9) Are there any form requirements imposed on the party from the other country?	There is no discrimination among citizens of different EU Member States. The international private law must be applied for trans-national contract relationships.	No	?
9a) Are there different form requirements imposed on the party from the other country or are they applied in a different manner?	No **For European party the mutual recognition clause applies to the foreign certification authority**	No	?
9b) What are they and what is the public policy underlying such form requirements?	#	#	?

Note: BIAC inputs are added as **bold with underlines**

Questions	Norway	Sweden	Switzerland
6) Does your country have form requirements on contracts that depend on whether the transaction was completed by paper, hand written signatures, or electronic signatures?	No	Swedish Contracts Act: A contract can be concluded by oral or electronic means unless there is a specific regulation in another act prescribing a special form requirement. **(e.g. To purchase real estate and a couple of financial services)**	No, except for few exceptions.
6b) Nature of such requirements?	#	General.	The few existing form requirements are imperative.
6b) Origin of such requirements?	#	?	Most often they come from national law, less from regional.
7) Are there any statutes, regulations providing for form requirements in legal proceedings, of a technical or non-technical nature?	No	No	For some contracts the Code of Obligations establishes written form requirements.
7a) Nature of such regulations?	#	#	Imperative.
7)b) Origin of such regulations?	#	#	Most often they come from national law, less from regional.
8) If yes to Q7), will legal recognition be provided to individual contracting parties that agree to use electronic documents?	#	# **Since there are few requirements in civil law and especially in contract law parties are most of the time free to use electronic contracts. Where there are form requirements however this is not possible.**	Parties can contract freely unless there is not stated differently by law. The imperative nature of the existing form requirements exclude the use of authentication methods other than those prescribed.
9) Are there any form requirements imposed on the party from the other country?	No	No	Form requirements depend on the contract nature. Particular form requirements depend on international private law.
9a) Are there different form requirements imposed on the party from the other country or are they applied in a different manner?	No	No	If the contracting parties are in different countries, form has to be the one prescribed in those countries.
9b) What are they and what is the public policy underlying such form requirements?	#	#	See above.

Note: BIAC inputs are added as **bold with underlines**

Questions	Turkey	United Kingdom	United States
6) Does your country have form requirements on contracts that depend on whether the transaction was completed by paper, hand written signatures, or electronic signatures?	The validity of the contracts are not subject to any form requirements unless contrary is clearly specified by codes.	Legislation is currently being put in place to enable this to be done electronically.	No, except for some specific cases. **(1) the creation and execution of wills, codicils, or testamentary trusts;** **(2) adoption, divorce, or other matters of family law; or** **(3) the Uniform Commercial Code, as in effect in any State**
6b) Nature of such requirements?	?	?	?
6b) Origin of such requirements?	?	?	?
7) Are there any statutes, regulations providing for form requirements in legal proceedings, of a technical or non-technical nature?	No	No, but the electronic signature has to be in accordance with its legal definition.	**The Electronic Signatures Act creates an exception for the courts [many states with form requirements for real property, and testamentary acts (wills)].**
7a) Nature of such regulations?	#	#	?
7)b) Origin of such regulations?	#	#	?
8) If yes to Q7), will legal recognition be provided to individual contracting parties that agree to use electronic documents?	#	In general, legal recognition will be provided.	**To the extent that public policy is not violated, recognition is generally possible. The principle is party autonomy is preserved in the Uniform Electronic Transaction Act (UETA) among other relevant and authoritative sources.**
9) Are there any form requirements imposed on the party from the other country?	No	No	No **Where notarisation is needed, a requirement to authenticate the notarial act via the use of an Apostille or otherwise. ***
9a) Are there different form requirements imposed on the party from the other country or are they applied in a different manner?	No	No	No * **The Electronic Signatures Act includes a notarial provision that may terminate such form requirements.**
9b) What are they and what is the public policy underlying such form requirements?	#	#	#**The public policy issue in requiring authentication via these paper requirements is intended to prevent fraud.**

Note: BIAC inputs are added as **bold with underlines**

Questions	**EU**	**BIAC**
6) Does your country have form requirements on contracts that depend on whether the transaction was completed by paper, hand written signatures, or electronic signatures?	**The present Directive does not apply to the harmonisation of Member States rules concerning contract law, particularly the formation and the performance of contracts, or other formalities of non-contractual nature concerning signatures.**	*The BIAC report provides additional information on: EU, CANADA, GERMANY, ITALY, SWEDEN, US*
6b) Nature of such requirements?		See above.
6b) Origin of such requirements?		See above.
7) Are there any statutes, regulations providing for form requirements in legal proceedings, of a technical or non-technical nature?		*The BIAC report provides additional information on: CANADA, ITALY, SWEDEN, US*
7a) Nature of such regulations?		See above.
7)b) Origin of such regulations?		See above.
8) If yes to Q7), will legal recognition be provided to individual contracting parties that agree to use electronic documents?		*The BIAC report provides additional information on: CANADA, ITALY, SWEDEN, US*
9) Are there any form requirements imposed on the party from the other country?		*The BIAC report provides additional information on: CANADA, GERMANY, ITALY, SWEDEN, US*
9a) Are there different form requirements imposed on the party from the other country or are they applied in a different manner?		See above.
9b) What are they and what is the public policy underlying such form requirements?		See above.

Note: BIAC inputs are added as **bold with underlines**

ANNEX 6: SUMMARY TABLE: SURVEY ON FORM REQUIREMENTS / FINANCIAL SERVICES

Questions	Australia	Austria	Canada
10) Are there any form requirements applicable to transactions in financial services?	Yes. The applicable legislation is: Corporations Law; Superannuation Industry (Supervision) Act 1993; Insurance Contracts Act 1984; Life Insurance Act 1995	No. There are only legal form requirements of writing with respect to consumer credit contracts or for bank accounts. However these form requirements do not influence contract validity.	There are some federal and provincial statutes that require that certain disclosures and contracts in respect of the enumerated topics be in writing.
10a) If yes to Q10), please specify the nature of the requirement.	Mandatory	?	Mandatory
10b) If yes to Q10), please specify the origin of the requirement.	Commonwealth and State Legislation	?	Federal and Provincial laws
11) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in financial transactions?	There is no specific legislation. The legislation referred to in Question 10 is currently outside the Electronic Transactions Act 1999. However, the general policy is to permit electronic commerce as long as it is lawful and there is no regulatory detriment in doing so.	No, the general Electronic Signature Act is applicable.	The federal Personal Information Protection and Electronic Documents Act and its, as yet, unwritten regulations, may permit the federally regulated aspects of the above-noted dealings to be carried out electronically.
11)a) If yes to Q11), are there any technical or non-technical requirements specified?	No, in general the policy is technology neutral.	No, more than a "secure" electronic signature will not be necessary.	The Act authorises regulations to be made to permit services or dealings by departments electronically. The provincial legislation may permit the provincially regulated aspects of the dealings electronically.
11)b) If yes to Q11a), why are such technical requirements necessary?	#	#	#
12) If no to Q11), why are electronic signatures or electronic authentication mechanisms not accepted?	Written evidence of a contract might be required in some circumstances through the operation of legislation, especially local state legislation. As a result, some legal impediments to the use of electronic signatures exist in the case of certain contracts and where members of the private sector are communicating with Government.	#	#
12)a) If no to Q11), are there any statutes, regulation or other norms that allow parties to vary these requirements among themselves by agreement of the parties?	?	No, but in principle, any arrangement would be possible and valid.	#
12)b) If no to Q11), are there any restrictions to the rights of parties to choose the proper forms of technology for a given transaction?	No, in general the policy is technology neutral.	See above	#
13) Does the usage of electronic signatures or electronic authentication mechanisms have the same legal consequences as paper written or hand signed documents under your country's from requirements in Q10?	Yes	Yes, under the condition that the employed mechanism is "secure".	The federal Personal Information Protection and Electronic Document Act permits the use of electronic signatures and electronic documents to comply with federal requirements. Legislation enacted in one province and proposed in four others would give electronic signatures and electronic documents the same legal consequences.
13)a) If no to Q13), please give reference information as to how different legal consequences are under them and why.	#	#	Note: BIAC inputs are added as **bold with underlines**

Questions	Czech Republic	Finland	Germany
10) Are there any form requirements applicable to transactions in financial services?	Yes. In the Commercial Code concerning Employee Stock Purchases, in the Banking Act, and the Stock Exchange Act. Some of these are related to budget rules and tax laws.	Yes. There is numerous legal statutes on form requirements in the field of financial services.	No. There are only legal form requirements of writing with respect to consumer credit contracts or for bank accounts. **Hand-written signatures on bills and checks, promotion of investments (prospectus)***
10a) If yes to Q10), please specify the nature of the requirement.	?	?	The contracts in question are not valid.
10b) If yes to Q10), please specify the origin of the requirement.	?	?	***Brokerage and Stock Trading in general is done informally and would not work if form requirements were imposed**
11) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in financial transactions?	The Electronic Signature Act, which is under consideration, will generally be applicable.	No	General Signature Law Act is applicable.
11)a) If yes to Q11), are there any technical or non-technical requirements specified?	?	#	Banking sector associations will ask for "secure" signatures and have worked out standards for smart card readers.
11)b) If yes to Q11a), why are such technical requirements necessary?	?	#	Security requirements
12) If no to Q11), why are electronic signatures or electronic authentication mechanisms not accepted?	?	?	
12)a) If no to Q11), are there any statutes, regulation or other norms that allow parties to vary these requirements among themselves by agreement of the parties?	?	?	Private arrangements within Banking sector is possible. See "Identrus" Project of some world leading banks. See. http://www.identrus.com/index2.htm
12)b) If no to Q11), are there any restrictions to the rights of parties to choose the proper forms of technology for a given transaction?	?	?	No.
13) Does the usage of electronic signatures or electronic authentication mechanisms have the same legal consequences as paper written or hand signed documents under your country's from requirements in Q10?	?	?	Yes, under the condition that the employed mechanism is "secure".
13)a) If no to Q13), please give reference information as to how different legal consequences are under them and why.	?	?	#

Note: BIAC inputs are added as **bold with underlines**

Questions	Italy	Japan	Korea
10) Are there any form requirements applicable to transactions in financial services?	**Intermediaries are allowed to offer financial services through Internet but they are required to observe rules concerning transparency**	Yes **Mandatory to draw a bill or a check in writing, prerequisite to make paper based documents to take mortgages, mandatory to make prospectus documents for investors, prerequisite for banks to accept a seal impression report from a customer**	No
10a) If yes to Q10), please specify the nature of the requirement.	**Recommendations adopted by the Italian Securities and Exchange Commission (CONSOB)**	Depending on the transaction, mandatory or prerequisite.	#
10b) If yes to Q10), please specify the origin of the requirement.	**Recommendations adopted by the Italian Securities and Exchange Commission (CONSOB)**	?	#
11) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in financial transactions?		**A ministry notifies banks to register customers' account numbers and PINs to use electronic authentication mechanisms in B-2-B and B-2-C Banking, and to stop handling if banks receive wrong PINs inputs**	Stock exchange: use of electronic document is permitted in case of submission to Financial Supervisory Committee (Stock Exchange Act). But there are no statutes, regulations or other norms in the other types of the transactions, except for the general provisions of the Digital Signature Act and the Basic Law on Electronic Commerce.
11)a) If yes to Q11), are there any technical or non-technical requirements specified?		?	There is no technical or non-technical requirement in Stock Exchange Law and its implementing law. In regard to the Digital Signature Act, there is some technical or non-technical requirement stipulated.
11)b) If yes to Q11a), why are such technical requirements necessary?		**to avoid transferring money by a request of a person who in fact doesn't have the right to do so.**	#
12) If no to Q11), why are electronic signatures or electronic authentication mechanisms not accepted?		?	#
12)a) If no to Q11), are there any statutes, regulation or other norms that allow parties to vary these requirements among themselves by agreement of the parties?		?	#
12)b) If no to Q11), are there any restrictions to the rights of parties to choose the proper forms of technology for a given transaction?		?	#
13) Does the usage of electronic signatures or electronic authentication mechanisms have the same legal consequences as paper written or hand signed documents under your country's from requirements in Q10?		**There are no rules about the usage of electronic signatures or electronic authentication mechanisms in many categories as described in Q.10. Formal legislation regarding electronic signatures, however, is expected to be effective on April 1st, 2001.**	Yes
13)a) If no to Q13), please give reference information as to how different legal consequences are under them and why.		?	#

Note: BIAC inputs are added as **bold with underlines**

Questions	Norway	Sweden	Switzerland
10) Are there any form requirements applicable to transactions in financial services?	Yes. The Financial Agreement Act entered into force on 1 July 2000.	Yes, many types of transaction. **Form requirements are mandatory in B-2-C lending. It is recommended in other B-2-C relations, but this has also to do with the fact that business has the burden of proof most of the time**	In most cases, there is no particular form requirements. Exceptions concern regulations against money laundering, some laws on banking supervision and consumer credit contracts.
10a) If yes to Q10), please specify the nature of the requirement.	The requirement that for example a consumer guarantee contract should be in writing is mandatory.	(*No general information*) The requirement that for example a consumer credit contract should be in writing is mandatory.	The existing form requirements are obligatory.
10b) If yes to Q10), please specify the origin of the requirement.	These requirements are, most often, a result of national law.	Most often, these requirements are a result of national law.	The existing form requirements derive from federal law. Bank-internal regulations and directives of banking associations play an important role, too.
11) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in financial transactions?	Yes	Electronic signatures and electronic authentication mechanisms are generally admissible unless there is a specific form requirement, as for example in the case of consumer credit contracts.	No, there is no specific regulations.
11)a) If yes to Q11), are there any technical or non-technical requirements specified?	No. It is only stated that one shall use "a secure method to be able to establish that the parties have entered into an agreement and the content of the agreement."	No	#
11)b) If yes to Q11a), why are such technical requirements necessary?	e.g. For Consumer guarantee contracts, to ensure that the signer is fully aware of the legal implications of such a contract/pledge.	#	#
12) If no to Q11), why are electronic signatures or electronic authentication mechanisms not accepted?	#	With respect to consumer credit contracts, the purpose of the form requirement, in addition to the value as evidence, is that the customer should be protected in that he will only make this kind of decisions after some consideration. This is also the reason for keeping the form requirement for the time being. **The law has not been changed**	This depends highly on the type of transaction. Most often, it is due to regional or specific legislation for a certain area. In the case of consumer credit contracts, the aim is to protect the consumer. In other cases, it can be the objective importance of the affair in question.
12)a) If no to Q11), are there any statutes, regulation or other norms that allow parties to vary these requirements among themselves by agreement of the parties?	?	No. There are no specific regulation or statutes that allow the parties to vary the requirements among themselves in financial transactions if it is B2C or G2C/B.	?
12)b) If no to Q11), are there any restrictions to the rights of parties to choose the proper forms of technology for a given transaction?	?	?	?
13) Does the usage of electronic signatures or electronic authentication mechanisms have the same legal consequences as paper written or hand signed documents under your country's from requirements in Q10?	It is not possible to give a yes or no answer to this. There acts and regulations that have already dealt with the issue as to whether electronic signatures can be accepted and given the same legal consequences as hand written signatures. However, this issue has not been addressed in many acts and regulations.	No. But it must however be noted that signatures or other means of authentication, are means of proof of the existence of a contract under Swedish law and does not themselves represent the conclusion of a contract. Thus, the value of a signature, both electronic and non-electronic, may be questioned as it may not fully represent the agreement between the parties.	Generally speaking: No. But the principle of free evidence means that they can eventually be given legal effect by the judge.
13)a) If no to Q13), please give reference information as to how different legal consequences are under them and why.	See above	See above	? (Note: BIAC inputs are added as **bold with underlines)**

Questions	Turkey	United Kingdom	United States
10) Are there any form requirements applicable to transactions in financial services?	?	No, in general this is left to the private sector. There is only few form requirements in: Consumer Credit Act 1974, Financial Services Act	*The USG notes the response from BIAC .***The ESIGGN law applies to nearly all types of commercial transactions, including banking, securities, insurance, mortgage lending, and retirement services, among others.**
10a) If yes to Q10), please specify the nature of the requirement.	?	Statutory (Consumer Credit Act) and non-statutory (Financial Services Act)	See above
10b) If yes to Q10), please specify the origin of the requirement.	?	?	**A single national legal standard for electronic contracts and signatures by pre-empting inconsistent state or federal laws.**
11) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in financial transactions?	No	Yes. The Finance Act 1999, enables the Inland Revenue and Customs and Excise to make regulations enabling the use of electronic communications for the delivery of information or the making of payments.	See above
11)a) If yes to Q11), are there any technical or non-technical requirements specified?	#	Electronic Communications, is defined as including "..any communications by means of a telecommunications system" (Telecommunications Act 1984).	See above
11)b) If yes to Q11a), why are such technical requirements necessary?	#	#	See above
12) If no to Q11), why are electronic signatures or electronic authentication mechanisms not accepted?	?	They are not accepted in case of non-conformity to its general definition, as stated above.	See above
12)a) If no to Q11), are there any statutes, regulation or other norms that allow parties to vary these requirements among themselves by agreement of the parties?	?	?	See above
12)b) If no to Q11), are there any restrictions to the rights of parties to choose the proper forms of technology for a given transaction?	?	?	See above
13) Does the usage of electronic signatures or electronic authentication mechanisms have the same legal consequences as paper written or hand signed documents under your country's from requirements in Q10?	No. Only written documents are accepted as legal document.	Yes	See above
13)a) If no to Q13), please give reference information as to how different legal consequences are under them and why.	?	#	Note: BIAC inputs are added as **bold with underlines**

Questions	EU	BIAC
10) Are there any form requirements applicable to transactions in financial services?	**By the proposed Directive on "Distance marketing of consumer financial services most of the financial services will be able to be delivered on-line with constraints on consumer protection and money laundering.**	*The BIAC response offers additional information on: EU, UK, US, CANADA, GERMANY, ITALY, JAPAN*
10a) If yes to Q10), please specify the nature of the requirement.		See above
10b) If yes to Q10), please specify the origin of the requirement.	**Exceptions mainly on estate credit or access to treasury bonds.**	See above
11) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in financial transactions?		*The BIAC response offers additional information on: CANADA, JAPAN, SWEDEN*
11)a) If yes to Q11), are there any technical or non-technical requirements specified?		See above
11)b) If yes to Q11a), why are such technical requirements necessary?		See above
12) If no to Q11), why are electronic signatures or electronic authentication mechanisms not accepted?		*The BIAC response offers additional information on: SWEDEN*
12)a) If no to Q11), are there any statutes, regulation or other norms that allow parties to vary these requirements among themselves by agreement of the parties?		See above
12)b) If no to Q11), are there any restrictions to the rights of parties to choose the proper forms of technology for a given transaction?		See above
13) Does the usage of electronic signatures or electronic authentication mechanisms have the same legal consequences as paper written or hand signed documents under your country's from requirements in Q10?		*The BIAC response offers additional information on: CANADA, JAPAN, SWEDEN*
13)a) If no to Q13), please give reference information as to how different legal consequences are under them and why.		See above Note: BIAC inputs are added as **bold with underlines**

ANNEX 7: SUMMARY TABLE: SURVEY ON FORM REQUIREMENTS / TRANSPORTATION AND DELIVERY SERVICES

Questions	Australia	Austria	Canada
14) Are there any form requirements applicable in the different categories of transportation transactions?	No, but most transport companies comply with the United Nations Lay Out Key.	A letter of Delivery has to contain the signature of the sender.	Carriage of Goods by Waters Act (COGWA) and the Bills of Lading Act.
14a) If yes to Q14), specify the nature of the requirement.	#	?	The COGWA provides that the "Hague-Visby Rules" have force of law in Canada
14b) If yes to Q14), specify the origin of the requirement.	#	National law	National law
15) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in transactions in transportation services specifically?	No. The general Electronic Transaction Act and the Uniform Transactions Bill are applicable.	No. The general Electronic Signature Act is applicable.	The COGWA and the Bills for Lading Act do not contain specific provisions regarding the use of electronic means. The development, acceptance and use of electronic documents in the transportation sector is in its infancy and the decision for the use and acceptance remains primarily with the contracting parties.
15)a) If yes to Q15), are the technical or non-technical requirements specified?	No, but the minimum standards set out in the UNCITRAL Model Law have to be respected.	No, more than a "secure" electronic signature will not be necessary.	#
15)b) If yes to Q15)a), why are such technical requirements necessary?	#	#	#
16) If no to Q15), why are electronic signatures not accepted?	#	In principle every arrangement would be valid.	#
16)a) If no to Q15), are there any statutes, regulations or other norms that allow contracting parties to vary these requirements among themselves by agreement of the parties?	#	#	#
16)b) If no to Q15), are there any restrictions to the rights of parties to choose the proper forms or technology for a given transaction?	No	#	#
17) Do electronic signatures have the same legal consequences as paper written or hand signed documents in transportation services?	Yes	Yes. All contracts and declarations are subject to the provisions of the Electronic Signature Act.	Yes?
17)a) If no to Q17), how different are legal consequences under them and why?	#	#	Note: BIAC inputs are added as **bold with underlines**

Questions	Czech Republic	Finland	Germany
14) Are there any form requirements applicable in the different categories of transportation transactions?	Yes. Goods import manifest, Import customs declaration, Export customs declaration, Transit declaration.	International transport: Yes, for example Bill of Lading. Moreover, there are requirements in the EC Customs Regulation.	A letter of Delivery has to contain the signature of the sender.
14a) If yes to Q14), specify the nature of the requirement.	?	Depending on the type of transaction, mandatory or non-mandatory.	Handwritten signature
14b) If yes to Q14), specify the origin of the requirement.	National law	National Law and international agreements.	International Law and EU regulations; Customs regulations
15) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in transactions in transportation services specifically?	Yes. Electronic Signature Act and Czech Customs Code: All of the import/export customs forms can be replaced by electronic forms. In the case of transit, the forms in the Common Transit Procedure are currently being replaced by internationally agreed electronic messages.	?	No. The general Electronic Signature Act is applicable. As far as Custom formalities are concerned, EU Regulation needed
15)a) If yes to Q15), are the technical or non-technical requirements specified?	?	No, but EDIFACT message standard is widely in use.	No, more than a “secure” electronic signature will not be necessary.
15)b) If yes to Q15)a), why are such technical requirements necessary?	?	?	#
16) If no to Q15), why are electronic signatures not accepted?	#	?	#
16)a) If no to Q15), are there any statutes, regulations or other norms that allow contracting parties to vary these requirements among themselves by agreement of the parties?	#	Parties can have mutual agreements.	#
16)b) If no to Q15), are there any restrictions to the rights of parties to choose the proper forms or technology for a given transaction?	#	No	#
17) Do electronic signatures have the same legal consequences as paper written or hand signed documents in transportation services?	?	In road and air transport: Yes.	Yes
17)a) If no to Q17), how different are legal consequences under them and why?	?	#	#

Note: BIAC inputs are added as **bold with underlines**

Questions	Italy	Japan	Korea
14) Are there any form requirements applicable in the different categories of transportation transactions?	In customs operation, it is obligatory to use the forms provided for by Customs European regulation " " European regulation of actuation " . **Transportation documents (bill of lading, waybill, invoice and so on) are still issued in paper form.**	Yes, Dangerous Goods Exports, Declaration by exporters, Invoice, Manifest, **Bill of Lading, Sea Waybill. Almost all Export/Import procedures are processed by NACCS to facilitate custom procedures and non-governmental procedures. Using NACCS is not mandatory**	Yes. Intra-company logistics: No. B-2-B Commercial Trade and B-2-C Delivery of Goods: Yes in the case of Bill of Landing and Invoice by Commercial Law. Moreover, some regulations require written report at importation or exportation.
14a) If yes to Q14), specify the nature of the requirement.	Obligatory **At present, an initiative is being studied in the field of B2B to create a common network**	Mandatory	?
14b) If yes to Q14), specify the origin of the requirement.	European regulations	National law, cabinet order, regulations	National law
15) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in transactions in transportation services specifically?	No **A legislative mechanism to use electronic signatures and authentication has been introduced in Italy, but, at present, such a mechanism is not effectively implemented in the field of logistics.**	**The Acts on electronic signature will come into force on 1st April, 2001. Under the new Acts, Notary Public in Japan will authenticate electronic signatures. Private companies can also authenticate electronic signature. Licenses for authentication are not mandatory.**	Yes. Facilitation of Goods Distribution Act, Act on the Promotion of Office Automation for Trade, Act on the Infrastructure of Industrial and Energy Technology Foundation.
15)a) If yes to Q15), are the technical or non-technical requirements specified?	#		No
15)b) If yes to Q15)a), why are such technical requirements necessary?	#		#
16) If no to Q15), why are electronic signatures not accepted?	**Although electronic signature and electronic authentication will eventually be widely accepted, time is required for adaptation**		#
16)a) If no to Q15), are there any statutes, regulations or other norms that allow contracting parties to vary these requirements among themselves by agreement of the parties?	#		#
16)b) If no to Q15), are there any restrictions to the rights of parties to choose the proper forms or technology for a given transaction?	#		#
17) Do electronic signatures have the same legal consequences as paper written or hand signed documents in transportation services?	Yes. After the rules of the point 16 will be in force, electronic signature will have the same lawful value of the hand-written one	**Electronic Bill of Lading is not recognised as "document of title" in Commercial Code and is only recognised as a evidence of contract. Paper bill of lading is necessary for the title of goods. Electronic Waybill is not recognised in Commercial Code. But, legal consequences might be similar to paper**	Yes
17)a) If no to Q17), how different are legal consequences under them and why?	#		#

Note: BIAC inputs are added as **bold with underlines**

Questions	Norway	Sweden	Switzerland
14) Are there any form requirements applicable in the different categories of transportation transactions?	Yes. However, this is an area which is widely governed by common international law and regulations.	Intra-company logistics: No. Customs regulation: There are form requirements in the EC Customs Regulation that apply directly in Sweden. This regulation is in turn based on an international customs convention. Requirements exist as well in relation to Bills of Lading and Waybills .	Yes: National transportation contracts. Customs declaration, import declaration concerning agricultural products. No: International transportation contracts.
14a) If yes to Q14), specify the nature of the requirement.	?	Arbitrary	Imperative
14b) If yes to Q14), specify the origin of the requirement.	International agreements	National, but in relation to international transport based on international agreements.	National law
15) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in transactions in transportation services specifically?	Yes	Yes. Customs regulation: Swedish Customs Act. Generally, rules supporting the use of electronic transport documents exist in relation to air and sea transport as the underlying international agreements contain such rules. The opposite applies to railroad and road transport.	No. But a specific ordinance allows the use of electronic procedures after authorisation by the National Customs Administration, with few exceptions made for certain goods. Moreover, temporary admissions (as defined by the Istanbul Convention on Temporary Admissions) can be processed electronically.
15)a) If yes to Q15), are the technical or non-technical requirements specified?	No. It is only stated that one shall use "a secure method to be able to establish that the parties have entered into an agreement and the content of the agreement."	The electronic documents will have to fulfil the UN-EDIFACT standard for electronic documents.	Yes. The computer equipment has to conform to the standard set out by the National Customs Administration.
15)b) If yes to Q15)a), why are such technical requirements necessary?	#	Ensure compatibility between the computer systems of the importers with the system of the Customs Authority.	?
16) If no to Q15), why are electronic signatures not accepted?	#	#	In the cases where it is not accepted, the written form requirements aim at facilitating procurance of legal evidence.
16)a) If no to Q15), are there any statutes, regulations or other norms that allow contracting parties to vary these requirements among themselves by agreement of the parties?	#	No. The transportation rules are arbitrary and the parties can themselves agree on the use of e.g. electronic authentication methods.	?
16)b) If no to Q15), are there any restrictions to the rights of parties to choose the proper forms or technology for a given transaction?	#	#	?
17) Do electronic signatures have the same legal consequences as paper written or hand signed documents in transportation services?	It is not possible to give a yes or no answer to this. There acts and regulations that have already dealt with the issue as to whether electronic signatures can be accepted and given the same legal consequences as hand written signatures. However, this issue has not been addressed in many acts and regulations.	No. But it must however be noted that signatures or other means of authentication, are means of proof of the existence of a contract under Swedish law and does not themselves represent the conclusion of a contract. Thus, the value of a signature, both electronic and non-electronic, may be questioned as it may not fully represent the agreement between the parties.	Given that there is no overall legal prohibition to use electronic signatures in transportation services, their legal value is generally recognised.
17)a) If no to Q17), how different are legal consequences under them and why?	See above	See above	#

Note: BIAC inputs are added as **bold with underlines**

Questions	Turkey	United Kingdom	BIAC
14) Are there any form requirements applicable in the different categories of transportation transactions?	Yes. Customs import declaration, customs warehouse declaration, customs export declaration, transit declaration.	Intra-company logistics: No. B-2-B Commercial: Yes (Trade Cargo Report). B-2-C Delivery of Goods: Yes. C-2-C Shipments: Yes, in particular for declarations of dangerous goods.	*The BIAC response provides information on: Italy, Japan.*
14a) If yes to Q14), specify the nature of the requirement.	?	?	See above
14b) If yes to Q14), specify the origin of the requirement.	National law	Most often, they originate from international agreements.	See above
15) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in transactions in transportation services specifically?	Yes. There is an amendment regulation on customs procedures by computerised means, but no legislative arrangement.	Yes. The Finance Act concerning delivery of information related to Customs & Excise and Inland Revenue.	*The BIAC response provides information on: Italy, Japan.*
15)a) If yes to Q15), are the technical or non-technical requirements specified?	Yes, EDIFACT message standard.	?	See above
15)b) If yes to Q15)a), why are such technical requirements necessary?	?	?	See above
16) If no to Q15), why are electronic signatures not accepted?	#	Dangerous goods declaration must be on paper as they have to accompany the goods.	*The BIAC response provides information on: Italy.*
16)a) If no to Q15), are there any statutes, regulations or other norms that allow contracting parties to vary these requirements among themselves by agreement of the parties?	#	The requirements are laid down in international agreements and thus depend on them.	See above
16)b) If no to Q15), are there any restrictions to the rights of parties to choose the proper forms or technology for a given transaction?	#	?	See above
17) Do electronic signatures have the same legal consequences as paper written or hand signed documents in transportation services?	The current regulation of custom procedures is still not clear and conflicts with existing national legislation.	Yes	*The BIAC response provides information on: Italy, Japan.*
17)a) If no to Q17), how different are legal consequences under them and why?	?	#	See above

Note: BIAC inputs are added as **bold with underlines**

ANNEX 8: SUMMARY TABLE: SURVEY ON FORM REQUIREMENTS / GOVERNMENT SERVICES

Questions	Australia	Austria
18) What has been undertaken in order to proceed with the application of electronic authentication technologies in the delivery of government services and programmes to the public?	All appropriate services offered by the Federal Government to businesses and the general public should be available online by the end of 2001. Some mechanisms are in place to facilitate this commitment, as for example the enactment and operation of the Electronic Transactions Act 1999, the creation and operation of the Business Entry Point and other numerous government online facilities, the development and introduction of policies, standards, guidelines and other electronic service delivery and e-commerce enablers across government agencies, etc.	Electronic filing of lawsuits was introduced in 1989. Since 1997 a complete interaction by electronic means between court, lawyers and participants is being implemented. Moreover, a chip card will be replacing the medical aid check. making electronic signatures in the social security and healthcare sector admissible. In the financial sector, accountants and tax consultants are allowed to electronically interchange financial data with the competent administration. The road pricing system for truck traffic on highways is based on cryptographic authentication mechanisms.
19) Is there a policy on the nature of authentication that may be used by citizens and businesses in on-line dealings with the Government?	A Government Public Key Infrastructure, which entails the use of x.509 digital certificates in transactions between Federal government agencies and business clients, is being implemented. A digital certificate for more general use between businesses and government agencies is being developed. At this stage, there are no definite plans to develop classes of digital certificates for use by individuals, or for the wide use of electronic authentication technologies other than PKI by Government.	It is allowed to communicate with public authorities also online, if the competent public authority is equipped with the necessary technical means. If a handwritten signature is required for a particular document, this requirement can be fulfilled by a secure electronic signature.
19)a) If yes to Q19), how is that policy delivered?	In the interests of adequate security, public confidence and inter-operability, the Australian Government requires all Commonwealth agencies to use Gatekeeper accredited service providers and products whenever using PKI based service delivery.	?
19)b) If yes to Q19), to what extent does the policy allow foreign authentication services to be used by your citizens and businesses?	There is no limitation on the use of authentication services originating in other countries by Australian citizens and businesses. The requesting party must however have a place of business in Australia.	?
19)c) If yes to Q19), to what extent has that policy been developed in conjunction with authentication service vendors and user representatives?	Service and product vendors and user representatives have participated throughout in the development of the GPKI and the design of accreditation guidelines and digital certificates.	?
20) Are there any form requirements applicable in the different categories of government services?	Yes. Many Commonwealth, State and Territory laws still require a wide variety of regulatory and fiscal transactions to be in writing, sometimes prescribing a particular format and delivery channel.	Yes. G-2-B: Procedure for public procurements requires different declarations and information in writing. G-2-B VAT: A written bill is required. Other: Certain applications (e.g. issuance of a driving license or a passport) require a handwritten signature.
20)a) If yes to 20), specify the nature of the requirement.	?	Mandatory
20)b) If yes to 20), specify the origin of the requirement.	Federal, State and Territory Law.	National law
21) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in the different government transactions specifically?	Yes. Recent Commonwealth tax reform legislation requires certain business entities to furnish GST (VAT) tax returns online. Generally speaking, the Electronic Transactions Act 1999 recognises electronic transactions and signatures, but will not apply to particular transactions until these are prescribed by regulation.	The general Electronic Signature Act is applicable.
21)a) If yes to Q21), are there any technical or non-technical requirements	Yes. PKI structure.	No
21)b) If yes to Q21), why are such technical requirements necessary?	In the interests of adequate security, public confidence and inter-operability.	#
22) If no to Q21), why are electronic signatures not accepted?	#	#
22)a) If no to Q21), are there any statutes, regulations or other norms that allow parties to vary these requirements by mutual agreement?	#	#
22)b) If no to question Q21), are there any restrictions to the rights of parties to choose the proper forms or technology?	#	#

Note: BIAC inputs are added as **bold with underlines**

Questions	Belgium	Canada
18) What has been undertaken in order to proceed with the application of electronic authentication technologies in the delivery of government services and programmes to the public?	All appropriate services offered by the Federal Government to businesses and general public should be available by the end of 2001. The details concerning this e-government project are not available at his time since they are still in discussion at high political level.	The federal Personal Information Protection and Electronic Document Act sets out various documents, the electronic alternatives to which secure electronic signatures must be attached, e.g. documents required by federal law to be in their original form, documents required by federal law to be under oath, and signed documents required by law to be witnessed. Therefore, the Act permits the use of electronic authentication technologies to enhance the delivery of government services and programs to the public, by permitting secure electronic signatures to be used in certain dealings with the Federal Government.
19) Is there a policy on the nature of authentication that may be used by citizens and businesses in on-line dealings with the Government?	?	Please note the actual technology which will qualify as secure electronic signatures has not been defined yet as the regulations under the Act have not been written yet. There will be a consultation period with interested parties (possibly including authentication service vendors and, likely, user representatives) prior to being finalised.
19)a) If yes to Q19), how is that policy delivered?	?	See 19)
19)b) If yes to Q19), to what extent does the policy allow foreign authentication services to be used by your citizens and businesses?	?	See 19)
19)c) If yes to Q19), to what extent has that policy been developed in conjunction with authentication service vendors and user representatives?	?	See 19)
20) Are there any form requirements applicable in the different categories of government services?	?	The federal Personal Information Protection and Electronic Document Act permits the use of electronic authentication technologies to enhance the delivery of government services and programs to the public, by permitting secure electronic signatures to be used in certain dealings with the Federal Government. The Act authorises regulations to be made to permit services or programs, which are designated by departments, to be delivered electronically. In addition, the legislation enacted in one province and proposed in four may permit any provincially regulated aspects of the dealings set out in question 20 to be carried out electronically.
20)a) If yes to 20), specify the nature of the requirement.	#	
20)b) If yes to 20), specify the origin of the requirement.	#	
21) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in the different government transactions specifically?	?	See 20) **Until the regulations under the Act are passed, it is not known whether the transactions will be permitted to be electronically. In addition, the proposed regulations which three provinces have introduced may permit any provincially regulated aspects to be carried out electronically.**
21)a) If yes to Q21), are there any technical or non-technical requirements	#	See 20)
21)b) If yes to Q21), why are such technical requirements necessary?	#	See 20)
22) If no to Q21), why are electronic signatures not accepted?	#	#
22)a) If no to Q21), are there any statutes, regulations or other norms that allow parties to vary these requirements by mutual agreement?	#	#
22)b) If no to question Q21), are there any restrictions to the rights of parties to choose the proper forms or technology?	#	#

Note: BIAC inputs are added as **bold with underlines**

Questions	Czech Republic	Finland
18) What has been undertaken in order to proceed with the application of electronic authentication technologies in the delivery of government services and programmes to the public?	Action Plan Projects for Information Literacy, Electronic Trade and Electronic Public Administration. The newly set up Office for Personal Data Protection will be charged with the tasks of the Central Certification Authority by October 2000.	There is already a well functioning system of national databases in place used by the national administration. All government offices are connected via IP networks. More than 100 different public sector pilot schemes and projects are currently being undertaken. The new official identity card will be enhanced by using smart-card technology.
19) Is there a policy on the nature of authentication that may be used by citizens and businesses in on-line dealings with the Government?	?	The Council of State made in 1998 a major decision-in-principle on electronic transactions, which laid the foundation for a comprehensive PKI infrastructure, providing generic services for electronic transactions with agencies. An important part of the PKI project is a new smart-card based national ID -card. The decision also includes setting up a X.500/LDAP public directory.
19)a) If yes to Q19), how is that policy delivered?	?	Act on the Openness in Government Acts (1999). stresses the importance of transparency in public affairs and sets new requirements to information management and information security.
19)b) If yes to Q19), to what extent does the policy allow foreign authentication services to be used by your citizens and businesses?	?	Following the European Union digital signature directive, a foreign certificate is accepted on the basis of the same criterions as the Finnish certificate.
19)c) If yes to Q19), to what extent has that policy been developed in conjunction with authentication service vendors and user representatives?	?	During the preparation of the Acts the comments of all service providers and associations of private sector were taken into account. The Electronic Identity Cards can be used by the private sector as well. All solutions are developed in the co-operation with other countries and private sector and are based in the open standards listed in the European standardisation EESSI report.
20) Are there any form requirements applicable in the different categories of government services?	There is form requirements for public bid procedures. Moreover, Excise duty and Customs Duty on import use SAD forms for declaration purposes.	?
20)a) If yes to 20), specify the nature of the requirement.	?	?
20)b) If yes to 20), specify the origin of the requirement.	National law	?
21) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in the different government transactions specifically?	Yes. The area of tax administration is governed by the Administration of taxes Act. Moreover, there is the Customs Code and the new Electronic signature act.	Yes. Act on Electronic Identity Card (1999) and the Act on Electronic Service in the Administration.
21)a) If yes to Q21), are there any technical or non-technical requirements	Yes	Yes, for electronic identification. Examples of standards used are: PKCS#15, X.509 and X.500.
21)b) If yes to Q21), why are such technical requirements necessary?	?	?
22) If no to Q21), why are electronic signatures not accepted?	#	An authority can accept digital signatures as long as the requirements of certificates and certificate authorities described in the Act on Electronic Administration are filled.
22)a) If no to Q21), are there any statutes, regulations or other norms that allow parties to vary these requirements by mutual agreement?	#	#
22)b) If no to question Q21), are there any restrictions to the rights of parties to choose the proper forms or technology?	#	#

Note: BIAC inputs are added as **bold with underlines**

Questions	France	Germany
18) What has been undertaken in order to proceed with the application of electronic authentication technologies in the delivery of government services and programmes to the public?	The majority of the administrative procedures are in any case partially (forms on line) electronically processed today. In particular, in declaration of VAT by the company, income tax return by the public, of social declaration by the company, as well as some sector of health and some custom, the steps are taken to accompany the use of electronic authentication technology for the processing of these procedures completely on line.	a) Legal infrastructure: Draft Law for the Public Services are under consideration in order to adapt the "Bundesverwaltungsverfahrensgesetz" and the "Verwaltungsverfahrensgesetze" of the German Länder. In the meantime some Länder have made "Preliminary Law" for pilot projects (i.e. City of Bremen and Baden-Württemberg). b) Realisation of use of signature: big number of pilot projects (http://www.dlr.de/IT/MM/media@komm/); Taxation "Pilot Project ELSTER: http://www.elster.de/; http://www.darmstadt.gmd.de/SPHINX/Aktuelles/index.htm; General Programm "Bund Online 2005" (http://www.bund.
19) Is there a policy on the nature of authentication that may be used by citizens and businesses in on-line dealings with the Government?	In a general, the companies or the public will need to use electronic certificates for online procedures. For the online declaration of VAT, a policy on certification standard has been introduced by the State (Ministry of Economy, Finance and Industry), on the base of format X509 v3. Certification authority is accredited for the delivery of certificate on company declarers. As of May 2001, the articles will be implemented. In the other fields in the same type like the income tax return or the declarations social, it is probable that the same type of procedure will be set up. In the sector of health, the authority of certification for the doctors is GIP CPS and each patient will receive soon a smart card of authentication containing a certificate.	Government PKI Infrastructure is in preparation: SPHINX (http://www.bsi.de/aufgaben/projekte/sphinx/index.htm)
19)a) If yes to Q19), how is that policy delivered?	The procedure of accrediting certification authorities is elaborated in accordance with the current norms and standards.	Planning phase
19)b) If yes to Q19), to what extent does the policy allow foreign authentication services to be used by your citizens and businesses?	No discrimination a priori	Planning phase
19)c) If yes to Q19), to what extent has that policy been developed in conjunction with authentication service vendors and user representatives?	The procedure of accreditation is elaborated in collaboration with the declaring companies, the administrative entities in charge of the management of the declarations and, in the field of the policy of certification as such, in collaboration with the European authorities of standardisation in the field of the electronic signature, like the EESSI.	Planning phase
20) Are there any form requirements applicable in the different categories of government services?		A general survey made by the Ministry of interior shows more than 3000 cases in different legal statutes**. In public procurement, civil law contracts are used. In general there is no form, but the authorities demand hand-written signatures. (In the future: electronic qualified signatures). Some specific statements have to be signed. Regarding taxation, the authorities do not have to sign the majority of their statements if they use electronic communication (and they do). In other areas form regulations exist from hand-written signature to authenticated documents.**
20)a) If yes to 20), specify the nature of the requirement.		
20)b) If yes to 20), specify the origin of the requirement.		
21) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in the different government transactions specifically?	Only the health sector is regulated for this purpose. In the other fields, they are the regulations of the procedures which fix or will fix the conditions relating to the electronic signatures used in online procedures.	No. The new draft Law for Public services will offer the general usage of electronic signatures
21)a) If yes to Q21), are there any technical or non-technical requirements	?	Under consideration
21)b) If yes to Q21), why are such technical requirements necessary?	?	
22) If no to Q21), why are electronic signatures not accepted?	Specific but not-discriminatory requirements (c.f. higher) concerning the necessary " quality " of the certificates. Except in the sector of health (smart card), no condition suitable for such or such procedure will be imposed on the devices for creation of electronic signature.	(Note: BIAC inputs are added as **bold with underlines**)

Questions	Italy	Japan
18) What has been undertaken in order to proceed with the application of electronic authentication technologies in the delivery of government services and programmes to the public?	Italy has issued a set of rules aiming to improve the quality of the services in Public Administration and citizens. - the administrative procedures and the rules for the right of access to administrative documents (Law No. 241/1990); - the reform of the Public Administration and the administrative simplification (Law No. 59/1997); - the simplification of the administration activities and the decisional and control procedures (Law No. 127/1997); - the electronic procurements; - the realisation of the Unitary Network of the Public Administration (RUPA); - the realisation of the electronic identity card; - the realisation of a system for the selection of PA providers (i.e. on-line auctions).	"Strategic Framework for Promoting Digitalisation of Administrative Procedures" was drawn up on 31 March 2000 in Japan. It set out key policies and programme for promoting on-line administrative procedures between the people and the government by FY2003, using electronic authentication technologies.
19) Is there a policy on the nature of authentication that may be used by citizens and businesses in on-line dealings with the Government?	See answer to Q6	Based on the fruits of experiment on cross-certification scheduled from January to March 2001, it will be developed.
19)a) If yes to Q19), how is that policy delivered?	See answer to Q6	
19)b) If yes to Q19), to what extent does the policy allow foreign authentication services to be used by your citizens and businesses?	See answer to Q6	
19)c) If yes to Q19), to what extent has that policy been developed in conjunction with authentication service vendors and user representatives?	See answer to Q6	
20) Are there any form requirements applicable in the different categories of government services?	Procurement/sales: European or national laws are applied according to the value of the transaction **There is a Government program to introduce electronic procedures in purchasing transactions and in payments by Public Authorities Electronic procurement is also taken into consideration by the European Commission in revising the EU directives on public procurement; member States should consequently comply with the rules defined at EU level when such rules will be approved. Electronic procurement is also on the agenda of the Trans-Atlantic Business Dialogue (TABD) in the 2000 program of co-operation between EU and US.** The subject of benefit claims is ruled by a set of norms for the various sectors. See also answer No. 21 as integration.	
20)a) If yes to 20), specify the nature of the requirement.	European or national laws are applied according to the value of the transaction	
20)b) If yes to 20), specify the origin of the requirement.	European or national laws are applied according to the value of the transaction	
21) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in the different government transactions specifically?	In addition to the Answer Q20,, regarding to the context of Ministry of Finance, the present rules allow the use of electronic authentication in order to officially send tax declarations, real estate lease contract registrations and tax payments ruled by norms issued by Ministry of Finance.	
21)a) If yes to Q21), are there any technical or non-technical requirements	Regarding to the context of Ministry of Finance, ruled by norms issued by Ministry of Finance	
21)b) If yes to Q21), why are such technical requirements necessary?	To allow the interoperability with final user systems and in order to guarantee: confidentiality of citizen personal data; integrity of transmitted data; authentication of citizens who pay taxes or their intermediaries; temporal certainty of the sent data (in relation to the deadline).	
22) If no to Q21), why are electronic signatures not accepted?	#	
22)a) If no to Q21), are there any statutes, regulations or other norms that allow parties to vary these requirements by mutual agreement?	#	
22)b) If no to question Q21), are there any restrictions to the rights of parties to choose the proper forms or technology?	#	

Note: BIAC inputs are added as **bold with underlines**

Questions	Korea	Netherlands
18) What has been undertaken in order to proceed with the application of electronic authentication technologies in the delivery of government services and programmes to the public?	The Digital Signature Act comprises the application of electronic authentication technologies in the delivery of governmental services and programs. Currently, there are 3 Certification Authorities designated which shall provide authentication service to governmental organisations and civil servants.	Although authentication technologies are not used on a large scale yet in the electronic delivery of governmental services to citizens, recently a project started to accelerate this development. It is the aim of performing 25% of the communication between governmental institutions, private sector and citizens in a secure electronic way in the year 2002. Many other pilots in this area are scheduled during 2000/2001.
19) Is there a policy on the nature of authentication that may be used by citizens and businesses in on-line dealings with the Government?	Studies are under way.	?
19)a) If yes to Q19), how is that policy delivered?	#	?
19)b) If yes to Q19), to what extent does the policy allow foreign authentication services to be used by your citizens and businesses?	#	?
19)c) If yes to Q19), to what extent has that policy been developed in conjunction with authentication service vendors and user representatives?	#	?
20) Are there any form requirements applicable in the different categories of government services?	Yes. In the area of G-2-B Procurement/Sales, the typical statute in this category is a law that has the government as the contracting party with regulations of writing and signature. G-2-B VAT: Law of value added tax. G-2-B Tax: Corporate tax law and Income tax law.	?
20)a) If yes to 20), specify the nature of the requirement.	Mandatory	?
20)b) If yes to 20), specify the origin of the requirement.	National law	?
21) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in the different government transactions specifically?	No	Tax: There is regulations allowing the payment of taxes by using PKI techniques.
21)a) If yes to Q21), are there any technical or non-technical requirements	#	?
21)b) If yes to Q21), why are such technical requirements necessary?	#	?
22) If no to Q21), why are electronic signatures not accepted?	It is planned to amend applicable laws to recognise the use of data message in those transactions.	#
22)a) If no to Q21), are there any statutes, regulations or other norms that allow parties to vary these requirements by mutual agreement?	Yes	#
22)b) If no to question Q21), are there any restrictions to the rights of parties to choose the proper forms or technology?	?	#

Note: BIAC inputs are added as **bold with underlines**

Questions	Norway	Portugal
18) What has been undertaken in order to proceed with the application of electronic authentication technologies in the delivery of government services and programmes to the public?	The Public Administration Network Project (1996), with a view to establishing a secure, trustworthy and effective communications infrastructure for the Norwegian public sector, comprising the cross-certification agreement (1999). A new task force has been appointed in February 2000, which has been charged with the task of outlining a PKI-policy for the public sector.	The need to review tax legislation and to promote the use of electronic data transfer within the public administration has been identified by the National Electronic Commerce Initiative.
19) Is there a policy on the nature of authentication that may be used by citizens and businesses in on-line dealings with the Government?	No	Principle 4 of the National Electronic Commerce Initiative stipulates free access to and circulation of encoding techniques.
19)a) If yes to Q19), how is that policy delivered?	#	Forms and information will be made accessible to the public free of charge or onerously.
19)b) If yes to Q19), to what extent does the policy allow foreign authentication services to be used by your citizens and businesses?	#	?
19)c) If yes to Q19), to what extent has that policy been developed in conjunction with authentication service vendors and user representatives?	#	The National Electronic Commerce Initiative recognises that the development of e-commerce is based on private initiative.
20) Are there any form requirements applicable in the different categories of government services?	Yes. Public Procurement Act, VAT Act, Unemployment declaration, Customs Act.	?
20)a) If yes to 20), specify the nature of the requirement.	?	?
20)b) If yes to 20), specify the origin of the requirement.	National law	?
21) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in the different government transactions specifically?	Yes. Customs Act Amendment 1997.	?
21)a) If yes to Q21), are there any technical or non-technical requirements	Yes. Compliance with standards is not mandatory. However, there is a standard requirements specification for TTP-services and digital signature, encryption products and services, based on SEIS, which contains both user-oriented and technical requirements and are upheld and updated in collaboration with the vendor sector.	?
21)b) If yes to Q21), why are such technical requirements necessary?	Standards are necessary for interoperability.	?
22) If no to Q21), why are electronic signatures not accepted?	The form requirements are mainly linked to the need to identify a person.	?
22)a) If no to Q21), are there any statutes, regulations or other norms that allow parties to vary these requirements by mutual agreement?	#	?
22)b) If no to question Q21), are there any restrictions to the rights of parties to choose the proper forms or technology?	#	?

Note: BIAC inputs are added as **bold with underlines**

Questions	Sweden	Switzerland
18) What has been undertaken in order to proceed with the application of electronic authentication technologies in the delivery of government services and programmes to the public?	Analysis on the Infrastructure and necessary organisational changes for the use of electronic mechanisms by and within the national administration (February and October 2000). Proposal for an Act on Qualified Electronic Signatures (May 2000), which will enter into force in January 2001. Public procurement of a framework agreement for services for electronic identification. **Some public authorities have started projects to enable citizens to communicate electronically with the help of electronic signatures.**	About 30 project: Switzerland is elaborating an appropriate PKI to be used by the public administrations. Also, the law on electronic signatures and the development of an electronic commerce application are under consideration. SmartCard certification options are examined as well.
19) Is there a policy on the nature of authentication that may be used by citizens and businesses in on-line dealings with the Government?	A general policy is currently being developed by the National Tax Board. It is e.g. suggested that certificates issued by the banks to be used in Internet banking, also shall be accepted in communication with the public sector.	No
19)a) If yes to Q19), how is that policy delivered?	?	#
19)b) If yes to Q19), to what extent does the policy allow foreign authentication services to be used by your citizens and businesses?	?	#
19)c) If yes to Q19), to what extent has that policy been developed in conjunction with authentication service vendors and user representatives?	In the study co-operation with vendor and user representatives will be considered in order to present a solution that is compatible with private sector solutions or plans.	#
20) Are there any form requirements applicable in the different categories of government services?	Yes. Procurement/Sales: Public Procurement Act. VAT and Tax: There are requirements on with respect to income tax returns, for social security and value added taxes, excise duties, as well as for decisions on tax matters. Benefit claims: There are over 40 different acts or regulations containing form requirements in the social insurance area.	Procurement/Sales: Yes, depending on the amount of money implied. TVA: No, only for reclamation. Tax: Yes. G-2-C: Yes.
20)a) If yes to 20), specify the nature of the requirement.	Regarding requests to participate, a confirmation of an electronic submission is mandatory.	?
20)b) If yes to 20), specify the origin of the requirement.	National law	National law, in the case of TVA central and regional law.
21) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in the different government transactions specifically?	Procurement/Sales: No. VAT/Tax: a security solution is under preparation that will be presented in October 2000. Benefit claims: a proposal for change to allow the use of electronic documents is presently out on a public hearing. The new regulations can enter into force no earlier than in January 2001.	Yes, for example for example in Tax area.
21)a) If yes to Q21), are there any technical or non-technical requirements	No	?
21)b) If yes to Q21), why are such technical requirements necessary?	#	?
22) If no to Q21), why are electronic signatures not accepted?	In the cases where electronic signatures or electronic authentication mechanisms are not accepted this is due to legislation.	#
22)a) If no to Q21), are there any statutes, regulations or other norms that allow parties to vary these requirements by mutual agreement?	?	#
22)b) If no to question Q21), are there any restrictions to the rights of parties to choose the proper forms or technology?	?	#

Note: BIAC inputs are added as **bold with underlines**

Questions	Turkey	United Kingdom
18) What has been undertaken in order to proceed with the application of electronic authentication technologies in the delivery of government services and programmes to the public?	Turkish Customs are supported by a computerised clearance system at Istanbul Airport. In 1999, the Ministry of Justice started an effort to make information on tax statuary available online.	Existing form requirements are being amended by the Electronic Communications Act in order to allow the use of electronic signatures in all areas. The Finance Act 1999 was changed to facilitate experiments into the VAT area. All government services will be available electronically by 2005.
19) Is there a policy on the nature of authentication that may be used by citizens and businesses in on-line dealings with the Government?	?	Two framework documents have been published, which adopt a non-discriminatory approach to authentication. Citizens and business will be able to acquire all kinds of credentials for various authentication purposes. The same policy applies to SmartCard Services. Moreover, all services should provide multilingual access and facilitation for citizens with impaired vision.
19)a) If yes to Q19), how is that policy delivered?	?	This is achieved by permitting authentication services to be provided by a range of different Trust Service Providers.
19)b) If yes to Q19), to what extent does the policy allow foreign authentication services to be used by your citizens and businesses?	?	The EU Electronic Signature Directive creates the framework for the acceptance of authentication from countries outside UK. In other cases, the government needs to have an appropriate degree of confidence in the identity of the counterpart.
19)c) If yes to Q19), to what extent has that policy been developed in conjunction with authentication service vendors and user representatives?	?	There is the industry-led co-regulatory *tScheme*, which is the principal accreditation / approval body.
20) Are there any form requirements applicable in the different categories of government services?	?	G-2-B Procurement/Sales: No. G-2-B VAT: Yes, related to the VAT registration and the VAT return itself (Value Added Tax Regulation 1995). G-2-B Tax: Yes, but some forms are also available electronically. B-2-C: Yes.
20)a) If yes to 20), specify the nature of the requirement.	?	?
20)b) If yes to 20), specify the origin of the requirement.	?	National law
21) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in the different government transactions specifically?	No	Yes. Value Added Tax (Amendment) Regulations 2000. The Customs & Excise body offers clearance services based on its own regulations.
21)a) If yes to Q21), are there any technical or non-technical requirements	#	Yes. For example the X.509 standard.
21)b) If yes to Q21), why are such technical requirements necessary?	#	?
22) If no to Q21), why are electronic signatures not accepted?	?	#
22)a) If no to Q21), are there any statutes, regulations or other norms that allow parties to vary these requirements by mutual agreement?	?	#
22)b) If no to question Q21), are there any restrictions to the rights of parties to choose the proper forms or technology?	?	#

Note: BIAC inputs are added as **bold with underlines**

Questions	**United States**
18) What has been undertaken in order to proceed with the application of electronic authentication technologies in the delivery of government services and programmes to the public?	In 1998, a Presidential Directive sets a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003. A report describes the Federal government's goals and efforts to develop a Public Key Infrastructure (PKI) to enable the widespread use of cryptographically-based digital signatures. The Memorandum "Electronic Government" (1999) called on Federal agencies to use information technology to ensure that governmental services and information are easily accessible. The "Government Paperwork Elimination Act" seeks to "preclude agencies or courts from systematically treating electronic documents and signatures less favourably than their paper counterparts".
19) Is there a policy on the nature of authentication that may be used by citizens and businesses in on-line dealings with the Government?	The final guidance maintains the basic policy of technology neutrality for automated transactions while recognising that agencies should select the appropriate technology relative to the risk of the application. **More information may be obtained by examining the 1999 Bill on Paper Work Reduction and Federal Documentary Requirements.**
19)a) If yes to Q19), how is that policy delivered?	The guidance and official USG policy calls on agencies to consider all of the available electronic signature technologies (including the advantages of public key technology) as part of their assessments.
19)b) If yes to Q19), to what extent does the policy allow foreign authentication services to be used by your citizens and businesses?	?
19)c) If yes to Q19), to what extent has that policy been developed in conjunction with authentication service vendors and user representatives?	?
20) Are there any form requirements applicable in the different categories of government services?	G-2-B Procurement/Sales: The basic rules that govern federal procurement can be found in the Federal Acquisition Regulations (FAR). VAT: There is no VAT at federal level. G-2-B Tax: Payment methods are very flexible. B-2-C including benefit claims: In general, no.
20)a) If yes to 20), specify the nature of the requirement.	?
20)b) If yes to 20), specify the origin of the requirement.	Depending on the context, most often state law, sometimes federal law.
21) Are there any statutes, regulations or other norms that recognise the use of electronic signatures in the different government transactions specifically?	Yes. Government Paperwork Elimination Act.
21)a) If yes to Q21), are there any technical or non-technical requirements	No
21)b) If yes to Q21), why are such technical requirements necessary?	#
22) If no to Q21), why are electronic signatures not accepted?	#
22)a) If no to Q21), are there any statutes, regulations or other norms that allow parties to vary these requirements by mutual agreement?	#
22)b) If no to question Q21), are there any restrictions to the rights of parties to choose the proper forms or technology?	#

Note: BIAC inputs are added as **bold with underlines**