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

03-Aug-2004

English - Or. English

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

DSTI/ICCP/REG(2003)9/FINAL
Unclassified

Cancels & replaces the same document of 15 July 2004

Working Party on Information Security and Privacy

SUMMARY OF RESPONSES TO THE SURVEY OF LEGAL AND POLICY FRAMEWORKS FOR ELECTRONIC AUTHENTICATION SERVICES AND E-SIGNATURES IN OECD MEMBER COUNTRIES

www.oecd.org/sti/security-privacy

JT00167912

English - Or. English

FOREWORD

This report sets out the results of responses received from 22 member countries to the *Survey of Legal and Policy Frameworks for Electronic Authentication Services and E-Signatures in OECD Member Countries* which was issued for completion in July 2003. It is intended to provide an understanding of both gaps and commonalities across jurisdictions with differing legal and regulatory approaches to electronic signatures.

The report was prepared by Canada, assisted by the OECD Secretariat and with active input and comments from member countries. It was declassified by the Committee for Information, Computer and Communications Policy on 2 July 2004.

This report is published on the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

SUMMARY OF RESPONSES TO THE SURVEY OF LEGAL AND POLICY FRAMEWORKS FOR ELECTRONIC AUTHENTICATION SERVICES AND E-SIGNATURES IN OECD MEMBER COUNTRIES

Purpose and objectives

The purpose of this survey is to identify both gaps and commonalities across jurisdictions with differing legal and regulatory approaches to electronic signatures to attempt to define mechanisms by which parties can use electronic signatures across jurisdictions. The survey was designed to be conducted in a manner coherent with that undertaken within Asia-Pacific Economic Cooperation (APEC) in order to allow for wider comparison. Its completion was expected to provide information on OECD member country legal and policy frameworks for electronic authentication and on regulations applicable to entities providing authentication services. On this basis, the exercise was intended to help determine how varying legislative/legal/policy frameworks can be "bridged" to provide for cross-jurisdictional acceptance of authentication services and for legal effect of electronic signatures. It was anticipated that part of the exercise may include the further identification of legal and regulatory barriers to electronic authentication that prevent the recognition of electronic signatures across jurisdictions in a non-discriminatory manner. Possible subsequent phases of this work could aim at identifying and assessing gaps in technical and operational approaches (*e.g.* guidelines, practices, security standards, etc.).

Terminology

For the purposes of this document:

- **Authentication services** include the elements involved in managing certificates, such as directory services and registration services, as applicable. The use of this term in this survey covers all these elements regardless of whether they are carried out by a single, or several, parties.
- **Licensing/approval** of authentication services (or service providers) is a certification/ approval/accreditation of services (or service providers) by evaluators that may involve, but is not limited to, bodies accredited by the government.
- **Electronic signatures** are passwords, personal identification numbers (PINs), biometrics, and other technologies, including digital signatures, used to establish the identity of the originator of an electronic message or document (the "signatory") and to indicate the signatory's approval of the message or document. An electronic signature or an electronic message or document bearing an electronic signature should not be denied legal effect simply because it is in electronic form.

Survey structure and content

The survey was broken down into three parts and contained questions related to each of the following areas:

- **Part I**: Domestic legal framework for authentication services and electronic signatures.
- **Part II:** Policies related to authentication services and e-services based in other jurisdictions.
- **Part III**: Operational-related policies.

For each question, respondents were requested to provide responses in the context of both the public and private sectors. The survey questions are attached to this document as Annex A.

Survey responses

Responses were received from 22 OECD member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Hungary, Italy, Japan, Korea, Mexico, Netherlands, Norway, Slovak Republic, Spain, Sweden, Switzerland, United Kingdom and the United States. A chart summarising the information provided by each respondent on key elements of each section of the questionnaire is attached as Annex B. It should be noted that this is a summary *interpretation* of the information provided.

General observations

This exercise appears to have been useful in terms of identifying areas where there are consistencies and those where there are inconsistencies and where future work could be focused. In this way, it can be used to develop a future work plan for the Working Party on Information Security and Privacy (WPISP) in the area of authentication and can be used to establish priorities for the various elements of that plan.

However, in going forward, it will be necessary to discuss the scope of the work and to determine if the public/private sector distinction is useful, necessary and viable. Additionally, while there was an attempt in this survey to ensure common usage of terminology, in any future work there will be a need to ensure that concepts are aligned so that the discussion can be meaningful and beneficial (*e.g.* the concepts of mandatory and voluntary schemes were not necessarily clearly distinguished and mutually exclusive in all cases in this survey. If this is to be a distinguishing factor in future work, there will be a need for greater specificity).

Depending on the objectives of future work, it may also be useful to make a distinction between electronic and digital signatures. The broad definition of electronic signature in the current survey was problematic in that most respondents found it necessary to make further breakdowns of the term in the context of their answers. This made comparisons of the information more difficult and subject to a greater degree of interpretation than is normally desirable in such surveys.

Finally, it should be noted that information considered in this analysis was as provided by respondents. If respondents did not describe certain aspects of their legislative framework (*e.g.* those that are known to exist in the case of European Union member states) there was no direct attempt to factor or impose that context into the response. As a result, the information contained in the summary chart may appear incomplete and may lack precision in some areas. More comparisons could have likely been made on a more direct basis if information on the full legislative context and framework had been provided.

Notwithstanding the above comments and observations, the survey produced findings of interest. These can be grouped into categories: areas where a high degree of consistency exists, areas where only some degree of consistency exists and finally, areas where there are inconsistencies. It is this latter area that will presumably be of greatest interest to the WPISP in defining its forward work plan in this subject area.

Highlights of findings

High degree of consistency

- ***Legislative/regulatory framework for e-signatures:*** Virtually all OECD member countries have some form of legislative/regulatory framework in place to provide for the legal effect of electronic signatures. While the specifics of the legislation differ, there would appear to be a high degree of consistency in approach and therefore the effect of the legislation.

- ***Licensing/accreditation/approval requirements for authentication services:*** Requirements do not exist in all cases. However, where an accreditation approach exists, the need for some form of approval or recognition of the service appears to depend on the scope of application and the type of authentication involved. More specifically where the authentication is for use by, or with, government agencies, some form of mandatory accreditation or recognition scheme exists in virtually all cases. Where a binding legal effect of the electronic signature associated with the service is the objective, there is, in virtually all cases, an accreditation scheme, often with some form of oversight or supervision involved.

- ***Technology neutrality:*** While all respondents indicated their legislative and regulatory framework for authentication services and e-signatures was technology neutral, the majority indicated that where e-government applications were involved, or where maximum legal certainty of the electronic signature was required, the use of technology that was asymmetric cryptography-based was specified. On this basis, while legislative frameworks may be technology neutral, policy decisions seem to require that the technology be specified. As such, it may be said that technology neutrality exists in theory, but not in practice.

- ***Secure e-government:*** Virtually all member countries indicated that secure electronic government was a priority. As indicated above, the majority indicated that a PKI-based solution is being implemented to address this priority. A smaller number indicated that they are partnering with the private sector and using their services for government requirements. In virtually all cases, mandated technical standards and policies exist for interactions among trust domains where at least one of the participants is a government entity.

- ***"Foreign"-based signatures and services:*** Legislative frameworks do not appear to deny legal effectiveness to signatures originating from services based in other countries as long as they are created under the same conditions as those given legal effect domestically. On this basis, the approach appears to be non-discriminatory as long as local requirements, or their equivalent, are met. This was generally the case with respect to authentication services themselves as well.

- ***Credential requirements:*** While the specifics of credential requirements varied, they were generally reported to be a function of the level of assurance sought and the degree of certainty of the legal effect to be accorded to the electronic signature.

Some consistency

- ***Registration processes:*** Registration processes and credential requirements were broadly comparable but differed on the question of whether existing or prior relationships between the authentication provider and the applicant could be used for the registration process. One respondent indicated that a distinction needed to be made between attribute authentication and identity authentication in this regard.

- ***Evaluation of services:*** There would appear to be some degree of consistency in the recognition of the need for some form of independent evaluation of entities providing authentication services. However, the nature and extent to which the requirements of such evaluations and those performing the evaluations were specified varied considerably (see below).

Inconsistencies

- ***Nature of audit requirements:*** The requirements for audit and compliance reviews varied significantly with some OECD member countries requiring mandatory audits annually and others having no requirements. Similarly, there were differences as to who was eligible to conduct the audits.

- ***Recognition of foreign authentication services:*** The focus of efforts appears to be on establishing frameworks for domestic services. Thus, mechanisms for recognising foreign authentication services are generally not very well developed.

- ***Technical standards:*** Inconsistencies appear to arise with respect to whether technical standards are mandated or not. There is also some inconsistency with respect to the use of internationally recognised standards (variations in national implementations in some cases and the use of stand-alone domestic standards in others).

Conclusions

The WPISP, through a series of inventories and now this questionnaire, has been addressing the subject of authentication for over five years. The information exchange to date has been valuable in terms of identifying commonalities and variances in member countries' approaches to authentication. This work establishes a good foundation for the WPISP to make strategic decisions about where it should focus future efforts to further existing global co-operation and collaboration in the area of authentication.

A preliminary discussion of the results of this survey and proposed next steps took place at the 15th meeting of the WPISP (15 October 2003). At that time, it was generally agreed that the overall, long-term objective of the WPISP's work in this area should continue to concentrate on exploring mechanisms for how the varying legislative/legal/policy frameworks can be "bridged" to provide for cross-jurisdictional acceptance of authentication services and for legal effect of electronic signatures. However, there was a view that, as a next step in addressing this objective, there is need to better understand the existing cross-border authentication marketplace. More specifically, there is a need to examine the usage of existing authentication offerings that are used across borders and identify the impediments and/or barriers these offerings are encountering.

This work would, in essence, be a further, practical, examination of member country approaches to "foreign" services. This survey has provided the WPISP with initial findings in this area suggesting that member countries run the risk of developing divergent approaches. While respondents indicated that, for the most part, there were no legal or regulatory barriers to electronic authentication that prevent the recognition of "foreign" electronic signatures in a non-discriminatory manner in their country, it is important to understand whether this is actually the case in practice. Shifting the focus of the WPISP's work to initiatives aimed at better understanding the current marketplace for cross-border authentication will provide important information about where future work should be focussed and the priority it should be assigned.

In this next stage of its authentication work, the WPISP should pay particular attention to drawing on UNCITRAL (United Nations Commission on International Trade Law) expertise gained during the course of developing the *Model Law on Electronic Signatures*. In all stages of its future work, the WPISP will need to take into account the discussions and work underway in various other international forums examining authentication issues (*e.g.* APEC). In this regard, it will be important to avoid overlap and duplication of effort and ensure that the WPISP benefits from the experience of these other forums and builds on their work.

ANNEX A

SURVEY OF LEGAL AND POLICY FRAMEWORKS FOR ELECTRONIC AUTHENTICATION SERVICES AND E-SIGNATURES IN OECD MEMBER COUNTRIES

I. Legal framework

For each of the following questions, please provide information in the following contexts:

- *Public sector; and*
- *Private sector (if different than public sector).*

1. Please name and provide a general description of any legal or policy framework you have that sets parameters for the establishment and operation of authentication services. ***Note****: If the legislation is broad and applicable on a multi-national or regional basis, it will be important to explain the impact of your country's legislation on extra-territorial issues.*

2. Is there a domestic licensing system in your country? If yes, is it mandatory for all those wishing to provide authentication services? If not, what are the benefits of being licensed? If no legislation exists and there is no licensing requirement, please describe any domestic framework that has been established for the operation of these services in your country.

3. What is the legal and policy framework within which electronic signatures operate? Is their legal effect established in domestic legislation and, if yes, how does it function? ***Note****: If the legislation is broad and applicable on a multi-national or regional basis, it will be important to explain your country's implementation of the legislation.*

II. Policies related to authentication services and e-signature based in other jurisdictions

4. If you have legislation and it includes provisions regarding the operation or use of authentication services based in other countries, please describe those provisions. If no legislation exists, are there other *non-legislative approaches that include provisions regarding the operation and use of authentication services based in other countries?* What are those? ***Note:*** *For example, are there government regulations under which the government authority may provide for the recognition of authentication providers based in other countries? Or are there requirements established for international agreements for foreign recognition?*

5. Are there application fees for authentication service providers from other jurisdictions wishing to be recognised in your country? Are there annual renewal fees and certification requirements involved? If so, are they different from domestic providers?

6. Does the legislation give legal effect to electronic signatures created outside your country on a non-discriminatory basis?

III. Operational-related policies

7. Are technical standards for the operation of authentication services mandated through domestic legislation or through any other formal arrangements? If yes, what are the internationally recognised standards?

8. What domestic or contractual requirements exist to ascertain the identity of the individual or organisation (the "applicant") seeking electronic credentials from an authentication service provider? What types of documentation and/or physical identification credentials are required?

***Note**: For example, are there requirements that the authentication method to verify the identity of the applicant be commensurate with the level of assurance accorded by the authentication process?*

Should face-to-face processes be employed to establish the identity of an applicant? Can a pre-existing trust relationship between the authentication service provider and the applicant be relied upon? Can the authenticity of attribute information of an applicant also be verified against official documents issued by the authorised organisations?

For authentication of organisations, some examples of means of verification include consulting the database of a service that identifies organisations or inspecting the organisation's articles of incorporation.

9. Are compliance audits required for licensed/recognised/accredited authentication service providers? If yes, what are the requirements for audits and who is qualified to undertake such audits? What is the required frequency? If no, is there a voluntary system in place?

10. Are the laws or policies governing authentication services and electronic signatures technology neutral?

ANNEX B

SUMMARY INTERPRETATION OF INPUT RECEIVED ON SURVEY OF LEGAL AND POLICY FRAMEWORKS FOR ELECTRONIC AUTHENTICATION SERVICES AND E-SIGNATURES IN OECD MEMBER COUNTRIES (MARCH 2004)

Part 1: Legal framework	Domestic authentication legislation/regulations?	Licensing or accreditation regime for authentication providers?	Legislation/regulations for legal effect of e-signatures?
Australia	Yes.	Public Sector: Accreditation mandatory for PKI-based certificates used by and with government agencies. Private Sector: Nothing mandatory.	Yes.
Austria	Yes.	No licensing but notice requirement for certification service providers and requirement to submit security and certification policies. Those offering qualified certs or secure electronic signatures must demonstrate adequate execution of security requirements of the Austrian Signature Act.	Yes. The Austrian Signature Law is an exact transition of the EU Directive for electronic signatures.
Belgium	Yes.	No licensing but notice requirement for service providers issuing qualified certificates.	Yes. "Qualified electronic signatures" fulfil form requirements.
Canada	Public Sector: Regulations federally. Addressed in legislation/regulations in one province. Private Sector: Voluntary principles have been established.	Public sector: Federally, no licensing but the tools of cross-certification and recognition are used to ensure policy and technical requirements are met. Regulations will recognise providers interacting with the federal government. Accreditation provided for legislatively in one province. Private Sector: No licensing but benchmarks for service established in principles.	Federal legislation exists for federal government form requirements. Legislation has been enacted at the provincial level to give legal effect to e-signatures in areas within their jurisdiction (*e.g.* contracts, consumer protection).
Czech Republic	National legislation implements the EC Directive. Decree focuses on the technical and procedural requirements of certification service providers.	Notice requirement for providers of qualified certificate. Voluntary accreditation designation is available.	Public sector: Yes if they are advanced e-sigs based on qualified certificates. Private sector: Yes, if agreed to by transacting parties.
Denmark	Yes. Act implementing the EC Directive on e-signatures.	No licensing regime but there is a notice requirement for providers issuing qualified certificates.	Yes. "Advanced electronic signatures" based on qualified certificates and secure signature creation devices fulfil form requirements.
Finland	Yes. The basic framework of authentication and electronic signatures for both the public and private sector is defined in legislation.	No licensing regime but notice requirements exist for issuers of qualified certificates.	Yes. Advanced signatures based on a qualified certificate created by a secure signature creation device (as per the EU Directive) fulfil signature requirements.
France	Yes.	Establishment and operation of authentication services is unrestricted and there is no licensing system but a voluntary "qualification of providers of certification services" scheme is being established for the issuance of qualified certificates.	Yes. Signatures created by a secure signature creation device, coupled with a qualified certificate issued by a qualified provider carry the same weight as a handwritten signature.

Part 1: Legal framework	Domestic authentication legislation/regulations?	Licensing or accreditation regime for authentication providers?	Legislation/regulations for legal effect of e-signatures?
Germany	Yes.	No mandatory prior accreditation but there is a notice requirement for those issuing qualified certs. Voluntary accreditation is possible.	Yes. "Qualified electronic signatures" fulfil form requirements for handwritten signatures.
Hungary	Yes. Legislation specifies "normal" (advanced) electronic signatures and "qualified" electronic signatures.	Any organisation can offer authentication services, but to issue legally binding certificates must be an advanced or qualified certification authority (submit CP and CPS to the authority).	Yes. "Advanced digital signatures" are equal to handwritten signatures and "qualified" ones are equivalent to witnessed signatures.
Italy	Yes. Legislation distinguishes between "electronic signatures", "digital signatures" and "user authentication".	Accreditation requirements depend on public/private sector application and type of authentication involved.	Yes.
Japan	Yes. Several pieces of legislation exist, each with a particular scope. A policy framework exists for government PKI.	Voluntary accreditation system available for private sector service providers.	Yes.
Korea	Yes.	Voluntary accreditation scheme exists. Accredited providers are regulated by legislation.	Yes.
Mexico	Federal law mandates that a record be kept of all entities providing public sector services. For the private sector, the Code of Commerce and associated regulations are relevant.	No.	Yes. Via the Federal Law of Administrative Procedure and, in the context of the private sector, via the Code of Commerce.
Netherlands	Legal implementation of EC directive on framework for electronic signatures in place. A policy framework exists for government PKI. No legal or policy framework for lower trust levels than typically associated with PKI.	For issuers of qualified certificates, no licensing obligation but there are notice requirements. A voluntary certification scheme is in operation for providers generally.	Yes. Legal effect is established equivalent to handwritten signatures based on a sufficient level of authentication.
Norway	Domestic legislation and regulations implement the EC Directive (with some national amendments).	No licensing system exists, neither as a legal mandatory requirement nor as a voluntary system.	No general evidential rules prohibit the use of electronic signatures on the sole grounds that they are electronic. Qualified signatures are given equivalent legal effect to handwritten signatures provided the law does not prohibit electronic communication in a given application area.
Slovak Republic	No special legislation. Services are performed according to international standards or the Act on Electronic Signatures (based on the EC Directive).	No.	Yes.
Spain	The EC Directive has been implemented in national legislation.	In accordance with the EC Directive, there is no licensing regime.	Yes, qualified signatures have the same legal effect as handwritten signatures; while other types of electronic signatures have a general recognition of their legal effect subject to the general rules on legal evidence.
Sweden	The EC Directive has been implemented in national legislation.	No.	Yes for qualified signatures. General principles of contractual freedom apply and e-sigs are recognised.
Switzerland	Yes, an ordinance and pending federal law apply to providers who choose to come under the framework.	No. Recognition of providers is optional. Recognition of providers is affected by an accredited certification body.	Currently written form is required by law for some contracts. However legislation recognising e-sigs is pending.

Part 1: Legal framework	Domestic authentication legislation/regulations?	Licensing or accreditation regime for authentication providers?	Legislation/regulations for legal effect of e-signatures?
United Kingdom	Yes. The legal framework exists at two levels: UK legislation and regulations (to meet EC Directive requirements).	No but existing legislation does provide for a statutory scheme for registration and approval of service providers. This part of the Act is not in force to allow for the private sector to meet the Act's objectives. A voluntary, industry-led scheme (*tScheme)* offers approval against industry agreed profiles.	Yes.
United States	Public sector: Legislation exists at the federal and state level. Federal government agencies are required to implement electronic processes by October 2003. Private sector: Legislation in place that validates the use of e-sigs in commercial transactions.	Federally, no licensing exists but cross-certification with the federal bridge is required for federal acceptance of external PKI credentials. The federal government is also developing capability for the federal acceptance of user-id/pin/password-based identity assertions.	Yes.

Part II: Policies re: services based in other jurisdictions	Parameters for operation of "foreign" authentication services established in legislation or policy?	Application fees?	Non-discriminatory legal effect to electronic signatures?
Australia	No.	No.	Yes.
Austria	Yes. Need to meet the requirements set out in domestic legislation that implements the EU Directive.	No application fees but fees for being listed in the Austrian directory of certification service providers. Also, fee involved if foreign service wishes to be accredited in Austria (voluntary).	Yes (as long as the requirements set out in the EU Directive are complied with and the validity of the qualified certificate can be verified from Austria.)
Belgium	Yes. Need to meet the requirements laid down in national regulation that implements the EU Directive.	No.	Yes.
Canada	Public sector: Processes for cross-certification are set out in published documentation. Private sector: The principles are silent on this matter.	No.	Yes.
Czech Republic	Czech legislation gives the same value to domestic and EU member state qualified certificates. Third countries must meet the parameters established in the EC Directive.	Yes for accredited providers. It is the same for domestic and foreign providers.	Yes. Legislation does not deny legal effectiveness to e-signatures from other countries.
Denmark	Yes for qualified certificates in accordance with the EC Directive only. No regulations exist for other types of e-signatures.	No.	Yes.
Finland	Yes. Must meet the same requirements as domestic providers defined in domestic legislation.	Yes. A registration fee exists for all issuers of qualified certificates to the public.	Yes according to conditions based on the EU Directive (with one additional option for certs of EU-based providers of qualified certs to be recognised as long as they meet the qualified cert requirements of that state – *i.e.* membership in "voluntary accreditation scheme not required".)
France	French legislation concerning the recognition of services based abroad is a direct transposition of European law. It is aimed at providers issuing qualified certificates.	No.	Yes.

Part II: Policies re: services based in other jurisdictions	Parameters for operation of "foreign" authentication services established in legislation or policy?	Application fees?	Non-discriminatory legal effect to electronic signatures?
Germany	As per the EC signature Directive, there are rules and technical requirements for foreign providers of qualified electronic signatures.	No.	Yes (as long as they meet the requirements set out in the EC Directive).
Hungary	No provisions currently but when Hungary joins the EU, all EU-based CAs will be accepted as domestic ones.	No.	Yes.
Italy	As per EC Directive, operations based in other member states are legally equivalent to domestic ones. Parameters for non-EU international operations are established in the Directive.	No.	Yes (under certain conditions in the case of "digital signatures"). Only with the European Community in the case of "user authentication".
Japan	Provision for CAs outside Japan to be accredited (procedure for accreditation is simplified under certain conditions).	Application and renewal fee for accreditation. It is the same for domestic and foreign providers.	Yes.
Korea	There is no legislation that limits the use of foreign services. However legal effect of e-signatures only possible where an agreement for reciprocal recognition exists.	No.	Yes, in cases where there is an agreement for reciprocal recognition.
Mexico	Yes, through provisions set out in the Code of Commerce.	No.	Yes, as is established in the Code of Commerce.
Netherlands	No legislation in place other than sector-specific applications and regulations. The government PKI can, under their policy, make use of services offered in other countries.	Annual registration/supervision fee for providers issuing qualified certificates to the public. Foreign providers may incur extra costs to be included in supervision activities.	Yes. In accordance with the EC Directive.
Norway	Legislation regulates certain international aspects. Certificates established within the European Economic Area are considered qualified if they meet the requirements for qualification within the country they were established.	No application fees for providers from other jurisdictions wishing to be recognised in Norway. However both domestic providers and foreign services must pay an annual registration fee if they wish to be registered with the NPT.	Yes, as a basic principle.
Slovak Republic	Foreign services can operate on the basis of an international agreement.	No fees for registration of domestic services. Application fee for accreditation which is the same for both domestic and international services.	Yes.
Spain	Yes. Need to meet the requirements set out in domestic legislation that implements the EC Directive.	No.	Yes. Legislation does not deny legal effectiveness to e-signatures from other countries (as per EC Directive).
Sweden	Yes for qualified certificates in accordance with the EC Directive only. No regulations exist for other types of e-signatures.	Annual registration/supervision fee for providers issuing qualified certificates to the public.	Yes.
Switzerland	Legislation will stipulate that providers recognised abroad under equivalent rules will be able to obtain recognition in Switzerland.	Possibly, but only for recognition assessments and subsequent audits.	Legislation is pending.

Part II: Policies re: services based in other jurisdictions	Parameters for operation of "foreign" authentication services established in legislation or policy?	Application fees?	Non-discriminatory legal effect to electronic signatures?
United Kingdom	Legislation does not contain provisions related to the country of origin of the service.	There are fees for granting and renewing approvals in *tScheme* (a voluntary industry-run scheme).	Yes.
United States	Federal public sector: The purchase of goods and services from foreign sources is regulated by the Federal Acquisition Regulations. Private sector: No parameters have been established by the federal government.	No application fees apply. The costs for testing for compliance to Federal Information Processing Standards (FIPS) must be borne by the product owner. There is no distinction made between domestic and foreign providers in this regard.	Yes.

Part III: Operational-related policies	Technical standards mandated? Internationally recognised standards?	Types of identification credentials required	Mandatory compliance audits? Frequency?	Are laws and regulations technology neutral?
Australia	Public sector: Various domestic and internationally recognised standards specified. Private sector: Identrus based on internationally recognised standards.	Evidence of identity requirements and process is a function of the level of assurance (a points system based on 4 levels of assurance). Examining possibility of making a distinction between "attribute" and "identity" authentication.	Public sector: Annual audits required.	Yes.
Austria	Yes. Technical requirements for providers of qualified certificates and secure signature creation devices are set out in the Austrian signature order. Requirements are based on EESSI/ETSI standards.	Identity requirements for qualified certificates, Official identity papers with photos are used. For public sector, an additional attribute (origin of signed document) is required.	Yes, start-up and every two years for issuers of qualified certificates. Auditors selected by the supervisory authority.	Yes, but when communication with public authorities is involved, certain functionality requirements must be met.
Belgium	No but must be compliant with the law and the EC Directive.	No requirements specified as of now. Providers use face-to-face.	Yes. Requirements currently being established.	Yes.
Canada	No but Government of Canada policies and technical specifications apply for interactions among trust domains where at least one of the participants is a federal government entity. The Principles reference internationally recognised standards.	Public sector: Face-to-face registration is required for medium/high assurance for federal government applications. Private sector: There are no national standards or contractual requirements to ascertain the identity of an applicant seeking electronic credentials.	Public sector: Providers recognised by the federal government will have compliance criteria to meet. Private sector: The Principles contemplate the need for independent compliance assessments.	Pubic sector: Legislation is technology neutral but enabling regulations at the federal level will be technology specific. Private sector: The Principles are expressed at a high level of generality and technology neutrality.
Czech Republic	Certain internationally-recognised standards are mandated at the decree level.	Two state-issued credentials required. Face-to-face not mandated.	Annual audits required.	Technology neutral in theory but not in practice.
Denmark	No technical standards specified in law. For advanced signatures internationally recognised standards specified in CP of National IT and Telecom Agency.	For qualified certificates "relevant" ID required that must contain name, address and social security number (or similar ID). Physical presence required if no existing/prior relationship.	Annual audits required.	Yes.

Part III: Operational-related policies	Technical standards mandated? Internationally recognised standards?	Types of identification credentials required	Mandatory compliance audits? Frequency?	Are laws and regulations technology neutral?
Finland	No technical standards are mandated through domestic legislation. International standards referenced for public sector communications.	Identity must be verified in a "careful and reliable manner". In practice, a face-to-face process is involved.	Supervision for compliance is the responsibility of a public authority that has the right to inspect hardware and software at any time.	Yes. Solutions based on PKI and qualified certs as well as other well-functioning methods are lawful.
France	French legislation does not impose any technical standards. European standards proposed as part of the voluntary system of certification.	Providers free to establish their own processes but face-to-face process will be required for qualified certificates.	Yes. Periodic audit required by an accredited independent body.	Yes but based on asymmetric cryptography-based standards.
Germany	The signature act and ordinance set out the technical criteria. The "Common Criteria" are integrated into the requirements.	ID requirements exist for qualified electronic signatures (as this is a core requirement for a secure signature service.) Possibility of using pre-existing trust relationships is being examined.	Yes. Every three years.	Rules are technology neutral apart from the fact that qualified electronic signatures rely on PKI.
Hungary	Yes. For advanced or qualified certificates. International standards have been taken into account in setting the requirements.	Identity checking is a function of the trust level.	Annual compliance audits are necessary for qualified CA providers.	Yes.
Italy	No mandatory standards for electronic signatures but technical standards exist for digital signatures and user authentication. Additional technical rules have been introduced for inter-operability purposes.	Depends on contractual agreements for electronic signatures but for digital signatures, face-face registration is required and prior trust relationships cannot be relied upon.	No compliance audit is required for electronic signatures or user authentication but audit requirements exist for digital signatures.	Yes (provided that the technology is asymmetric cryptography-based in the case of digital signatures and user authentication).
Japan	For public entities, technical standards mandated by ministerial ordinance & notifications. Domestic technical standards are mandated in legislation for accredited services. Standards are not specified for non-accredited services.	May be specified depending on application. Some require face-to-face. No exemptions for pre-existing relationships. No particular requirements imposed on non-accredited providers.	Provisions for inspection are stipulated for accredited providers. There are no specific requirements or rules for inspectors.	Public entities: PKI mandated. Private sector: technology neutral.
Korea	Internationally recognised standards are mandated for accredited CAs.	Credential requirements specified in regulations.	Audit requirements exist for accredited providers (six months after accredited date and annually thereafter).	Current laws and policies are technology neutral.
Mexico	Yes. Internationally recognised standards are referenced.	Means of verification of identity varies.	Not considered in the legislation.	Yes (since international standards are considered in their development).

Part III: Operational-related policies	Technical standards mandated? Internationally recognised standards?	Types of identification credentials required	Mandatory compliance audits? Frequency?	Are laws and regulations technology neutral?
Netherlands	Standards not mandated for generic authentication but are for government PKI. The standards are heavily based on EESSI deliverables. Detailed technical regulations can exist for sector-specific schemes.	Identity ascertained using official identity documents for qualified certificates and government PKI. Face-to-face required but pre-existing relationships can be relied upon under certain conditions.	No audit requirements in the supervision system. The voluntary accreditation scheme has compliance component (using accredited certification institutes).	At the level of the law and royal decree yes. At lower levels: no.
Norway	There are no references to standards in the Act or regulations. Recommendations for CPs for public sector use exist and are based on X.509 and the specs for qualified certificates.	Regulations exist with respect to qualified certs. Identity must be verified by personal appearance unless this has already been done through an existing customer relationship. Face-to-face process not required for certs at a lower trust level.	No since there is no licensing system.	Yes, as a basic principle. However, implementing legislation for the EC Directive is basically PKI.
Slovak Republic	Services are based on X.509.	"Definite" identifiers must be used.	Compliance audit is required annually for accredited providers. Auditor requirements are specified.	Legislation is digital signature-based.
Spain	No.	For qualified certificates, physical presence of the person is required or notarised identity documents can be submitted. However, some exceptions are permitted in case of previous accredited identifications.	No.	Yes.
Sweden	No.	Requirements exist for qualified certificates as per the Directive. More detailed requirements may be issued in the future.	No.	Yes.
Switzerland	The pending legislation provides for the Federal Council to develop provisions. The Council may not only consider international standards but make them directly applicable.	Face-to-face process generally required for qualified certificates. Not required for renewals though. Non-recognised providers are free to establish their own processes.	Yes for recognised providers. Recognition is valid for three years and partial audits are conducted annually.	Pending legislation will respect the principle of technology neutrality but the Ordinance only addresses digital signatures.
United Kingdom	Legislation does not mandate technical standards but evidence of compliance with standards may be required.	Registration process depends on level of assurance and whether government transactions are involved. Highest levels require face-to-face.	No legislative requirements for audits but *tScheme* requires annual audits.	Legislation is technology neutral but policy decisions of users are not technology neutral.

Part III: Operational-related policies	Technical standards mandated? Internationally recognised standards?	Types of identification credentials required	Mandatory compliance audits? Frequency?	Are laws and regulations technology neutral?
United States	Public sector: Federal authentication policy establishes technical requirements for each of four levels of assurance. Requirements for crypto processes are based on internationally recognised standards. Private sector: No standards mandated.	Public sector: Requirements to ascertain identities are still being defined. However, likely to be in-person requirement with official identification. Private sector: No stipulation.	Compliance audits required annually for inter-operability with the federal government.	Yes.