

Unclassified

DSTI/ICCP/REG(2005)4/FINAL



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

24-Nov-2005

English - Or. English

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

Working Party on Information Security and Privacy

THE USE OF AUTHENTICATION ACROSS BORDERS IN OECD COUNTRIES

**DSTI/ICCP/REG(2005)4/FINAL
Unclassified**

English - Or. English

JT00194846

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

FOREWORD

This report was presented to the Working Party on Information Security and Privacy (WPISP) at its 18th meeting in May 2005 and was declassified by the Committee for Information, Computer and Communications Policy (ICCP) at its 49th session in October 2005.

It was prepared by Jane Hamilton, from Industry Canada, based on input from OECD member countries and is published under the responsibility of the Secretary-General of the OECD.

Copyright OECD, 2005

**Applications for permission to reproduce or translate all or part of this material should be made to:
Head of Publications Service, OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France.**

REPORT ON THE USE OF AUTHENTICATION ACROSS BORDERS IN OECD COUNTRIES

Purpose and objectives

The purpose of this survey was to:

- Identify examples of current offerings and actual implementation of authentication across borders.
- Identify actual or potential barriers to the current cross-border use of digital signatures from the supplier/user perspective (taking into account input from other stakeholders as well).
- Explore the extent to which the cross-border offerings of authentication meet (or do not meet) transaction needs.

While the focus of this survey was on the current cross-border use of authentication methods/methodologies, it was also viewed as a good opportunity to collect information on factors that have been identified as fostering or impeding the national use of authentication technologies and digital signatures. On the basis that such information on national use of authentication would assist in understanding cross-border use, it was also collected.

The questionnaire was addressed to governments and to the private sector. Member countries were invited to supply examples of deployments of authentication technology in the public and/or the private sector in their country as they deemed suitable. This document is to be read in conjunction with input to the survey provided by the OECD Business and Industry Advisory Committee (BIAC) on behalf of members of the private sector that possess expertise related to the questions.

This survey is part of the ongoing work of the Working Party on Information Security and Privacy (WPISP) on authentication that is aimed at:

- Assessing the need to develop mechanisms to “bridge” varying legislative/legal/policy frameworks to provide for cross-jurisdictional authentication and for legal effect of electronic signatures.
- Promoting the use of authentication as an integral element of a safer, more secure Internet.
- Developing linkages so as to use the authentication work as an element for addressing other issues such as online identity theft, management of digital identities, spam, travel security, biometrics etc.

Scope

The scope of this survey is:

- Inclusive of both private and public sector authentication services.
- Inclusive of all transactions between government, business and individual users.

- Inclusive of all open systems, but including closed systems to the extent that they operate across jurisdictions. (Note: For the purposes of this discussion, “closed” involves a prior or existing relationship among the various parties involved in the authentication process.)
- Inclusive of all electronic authentication processes (making a distinction where legally valid signatures are involved, but being flexible enough to also accommodate solutions that do not use “signatures” in a narrow sense, like PIN-based solutions for example).
- Inclusive of all industry sectors (leaving the decision up to respondents to decide which ones to focus on).
- Focussed only on authentication of individual users (including business and/or government representatives), leaving other methods of authentication of machines to subsequent phases of work.
- Focussed only on authentication (setting aside authorisation).

Questionnaire structure and content

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

- **Section I:** Examples of cross-border authentication implementations.
- **Section II:** National uses of authentication technologies.

The questionnaire is attached to this document as **Annex II**.

Survey responses

Responses were received from 16 OECD member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Italy, Japan, Korea, Netherlands, Norway, Slovak Republic, and the United States. A table summarising the information provided by each respondent for each question is attached as **Annex I**. It should be noted that this is a summary *interpretation* of the information provided.

General observations

The utility of this exercise appears to have been somewhat limited owing to the disparate nature of the information collected. This was largely due to the fact that respondents were requested to provide examples of authentication implementations operating in their jurisdictions and were also at liberty to select the industry sector(s) upon which to base their response. This has made comparisons of the information difficult and subject to a greater degree of interpretation than is normally desirable in such exercises.

Another difficulty with the responses to this questionnaire was the lack of distinction made by respondents between those implementations that are offered on a cross-jurisdictional basis versus those that are national in scope. While the questionnaire distinguished between the two through its structure (*i.e.* Section I was cross-jurisdictional and Section II was national), respondents did not necessarily apply this distinction to their responses. Thus, there was a certain degree of ambiguity concerning the information provided, further contributing to the need for a greater degree of interpretation than is normally desirable.

However, despite the divergent nature of the information received, a number of common themes emerged from the responses that can be useful to the Working Party on Information Security and Privacy (WPISP) in validating, and further defining, its forward work programme on authentication. The information received will also have utility in terms of allowing the WPISP to establish priorities for the various elements of that programme.

Common themes

Positive

- ***Maturity and robustness of public sector implementations:*** Virtually all respondents included a description of at least one public sector implementation in their response. For the most part, these authentication offerings are robust (PKI-based) implementations that enjoy a reasonable degree of acceptance and success within their respective jurisdictions. In some cases, offerings do have a cross-jurisdictional scope (*e.g.* trade, customs, patents, health services) but these are limited. A number of respondents indicated that they are partnering with the private sector and using their authentication services for government applications. In virtually all cases, mandated technical standards and policies exist for interactions among parties where at least one of the participants is a government entity.
- ***Maturity of financial sector implementations:*** The majority of examples of authentication offerings described operate in the financial services sector. While most involve card-based online payments, others are extensions of online banking offerings and do not involve cards. A high degree of inter-operability appears to exist. This can likely be attributed to the homogeneous nature of the entities involved (*i.e.* virtually all involved regulated financial institutions) and the degree of standardisation, collaboration and co-operation in developing common infrastructures and platforms that is a tradition in this sector.
- ***Alignment of regulatory frameworks:*** All respondents reported that they have some form of legislative/regulatory framework in place to provide for the legal effect of electronic signatures at the domestic level. While the specifics of the legislation differ, there would appear to be a high degree of consistency in approaches in that most are based on existing international or transnational frameworks (*i.e.* the *European Directive 1999/93/EC on a Community Framework for Electronic Signatures* and the *UNCITRAL Model Law on Electronic Signatures*). On this basis, while not necessarily evident through concrete examples, it may be assumed that, at a general level, the legal effect that is accorded domestically would extend to the international community as well. However, this is an assumption based largely on theory and requires more “testing” in the marketplace, particularly with respect to the application of these frameworks to private sector offerings.
- ***Non-discriminatory approach to “foreign” signatures and services:*** The legislative frameworks do not deny legal effectiveness to signatures originating from services based in other countries as long as these signatures have been 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 is consistent with findings in previous WPISP surveys on authentication [cf. DSTI/ICCP/REG(2003)9/FINAL, DSTI/ICCP/REG(2001)10/FINAL, and DSTI/ICCP/REG(2000)1/REV1].
- ***Technology neutrality:*** While virtually all respondents indicated their legislative and regulatory framework for authentication services and e-signatures is technology neutral, the majority indicated that, where e-government applications are involved, or where maximum legal certainty of the electronic signature is required, the use of PKI is specified. On this basis, while legislative

frameworks may be technology neutral, policy decisions seem to require that the technology be specified. This is consistent with findings in previous WPISP surveys on authentication.

- ***PKI is alive and well:*** PKI is the authentication method of choice when strong evidence of identity and high legal certainty of the electronic signature is required. It is used in specific “communities of interest” where all users seem to have a prior business relationship of some form. The use of PKI-enabled smart cards and the integration of digital certificate functions into application software have made the use of this method less complicated for users. However, it is generally acknowledged that PKI is not required for all applications, and that authentication methods should be selected on a “fit-for-purpose” basis.
- ***All categories of users are engaged:*** While usage rates vary widely, with applications involving at least one government agency predominant, there is penetration across the user categories. As such, it can be concluded that a limited, but reasonably broad base of users of authentication services exists. This suggests that future communications initiatives pursued to promote authentication may have a degree of success that might not be enjoyed if an absolutely new, unknown concept were promoted in the marketplace.
- ***High degree of commonality on identity functionality:*** Virtually all applications and systems described provide evidence of identity. However, as one would expect, the strength of the evidence depends on the method of authentication used. Currently, the presumption of identity is strongest with PKI-based deployments.

Negative

- ***Interoperability:*** Challenges and limitations to interoperability are prevalent. At the technical level, although there is an abundance of standards, the lack of “core”, common standards for some technologies was cited as a problem. At the legal/policy level, the difficulty in principals understanding their respective trust framework, including assignment of liability and compensation, were cited as factors that are impeding progress. This is an area that would appear to require closer examination and scrutiny with a view to perhaps developing common tools to assist jurisdictions in achieving the level of inter-operability desired for a particular application or system.
- ***Recognition of foreign authentication services:*** The focus of efforts is on establishing domestic services. Thus, mechanisms for recognising foreign authentication services are generally not very well developed. On this basis, it would appear to be an area where further work would be useful. Given that any work in this area would be highly related to the more general subject of interoperability, the topics could be combined.
- ***Acceptance of credentials:*** In some cases, the acceptance of the credentials issued by other entities was cited as a barrier to interoperability. As such, consideration could be given to the possibility of developing a set of best practices or guidelines for issuing credentials for authentication purposes. Work may already be underway in several jurisdictions on this issue which could be useful input to any WPISP initiatives in this regard. Again, this could be an element of the inter-operability work item.
- ***A range of authentication methods in use:*** In virtually all OECD member countries, a range of authentication solutions is in use. The methods range from simple electronic signatures, passwords etc. on the one hand, to tokens, digital signatures and biometrics on the other. Depending on the application, and its requirements, the methods can be used alone, or in combination. While many would view this as positive, the information gathered in this survey suggests that the range of possibilities is so great that application providers and users run the risk of being hopelessly confused as to which method is appropriate for their requirements. This

would suggest that there could be some benefit to introducing a reference tool for assessing the various authentication methods and the degree to which their attributes address requirements identified by application providers and/or users.

- **Privacy-enhancing features:** The extent to which privacy considerations are being factored into implementations was not entirely clear from the information collected. Given the mandate of the WPISP, this may be an area of focus for future work as general research in this area indicates that the amount of personal information provided as part of an authentication process, and the privacy of that information, are significant issues for individuals.
- **Business cases for authentication:** While the questionnaire confirms that the use of authentication is growing, many respondents continue to cite the lack of defined business cases for authentication as an impediment. Defining the business case for authentication would have utility in communications initiatives promoting the use of authentication.
- **Absence of data on usage:** Data on usage was supplied by a limited number of survey respondents. However, the statistics provided lacked context, making the figures of limited use. Any future attempts to collect information of this nature should probably be done on a percentage basis (*i.e.* percentages of clients/customers/citizens utilising authentication services) to render more meaningful statistics. However, collecting additional data of this nature should be carefully assessed as it may only have utility in the context of measuring the effectiveness of campaigns promoting the benefits of authentication. This activity could be proposed to, and conducted in co-operation with the ICCP Working Party on Indicators for the Information Society (WPIIS) in the framework of the ongoing work on “indicators of trust”.

Conclusions and potential next steps

The WPISP, through a series of inventories, surveys and now this questionnaire, has been addressing the subject of authentication since 1998. This questionnaire represented an attempt to shift the focus of the work to initiatives aimed at better understanding the marketplace.

The information collected in this exercise has been useful in terms of identifying common themes that suggest future areas of work that could be given consideration by the WPISP. In summary form, these areas relate to:

- i.* Developing tools (*e.g.* guidelines, best practices, templates for developing agreements) to facilitate inter-operability, including aspects related to the acceptance of “foreign” services and certificates and the acceptance of the credentials of other service providers.
- ii.* Developing a framework for assessing the attributes of authentication methods so that they can be evaluated as to the degree to which they meet the requirements of a particular application. Such a framework could lend structure to the marketplace on both the supply and demand side. It would also be useful for researchers wanting to compare methods that are being used in the global marketplace. However, in undertaking any such project, it would be important to carefully define (and confine) the scope as well as the terminology utilised. It would also be important to reference the work on such frameworks already underway/completed in various member countries (*e.g.* France, United Kingdom, United States).
- iii.* Mapping the principles of fair information practices to the authentication environment. Such work could involve the articulation of measures to prevent the consolidation of transaction data and possibly guidelines for system designers to ensure their schemes do not include excessive requirements. (Note: This could have linkages to the framework for comparing authentication methods described above).

- iv. Undertaking initiatives aimed at defining the business case for authentication, in close co-operation with, and based on input from, the private sector.
- v. Undertaking initiatives aimed at promoting the use of authentication.

An assessment of the responses to the questionnaire also suggests that there are gaps in the information about the marketplace that should be filled. To address these gaps, future work undertaken could be aimed at *establishing a dialogue with those private sector entities providing authentication offerings on a cross-jurisdictional basis* with the aim of understanding, from their first-hand perspective, the barriers and impediments that they have had to overcome, or which continue to represent a challenge.

While BIAC input pursuant to this particular questionnaire may provide the type of information sought, establishing a direct dialogue with authentication providers may provide an opportunity for WPISP members to gain a better understanding of the cross-jurisdictional authentication environment. Such a dialogue could be a component of a future workshop or symposium convened to discuss the general need for a safer, more secure Internet. This could lead to the identification of specific, practical areas for the WPISP to focus its work.

If the dialogue was an element of a broader workshop agenda, it would also contribute to the WPISP's longer-term objective of *developing linkages between authentication and other elements of its forward work programme related to combating Internet threats*. It may also build on the linkage already identified in the context of spam, where the WPISP has agreed to reference results of possible work to be undertaken in the Spam Task Force on domain-level authentication.

Other areas where linkages could potentially be explored include assessing the extent to which authentication can play a role in combating identity theft, the extent to which the use of certain methods of authentication can alter the economic incentives for individuals to steal authentication credentials (*e.g.* through phishing schemes) and the promotion of authentication as an essential element of the OECD's culture of security.

However, in going forward with any work that involves promoting the increased use of authentication, the WPISP will need to remain mindful of the fact that there will be a corresponding increase in *the need for users to have ways to manage their digital identities*. If the WPISP decides to address this need, elements of the work would presumably include an assessment of the degree to which federated identity solutions can address marketplace needs in this regard, as well as an assessment of potential policy issues these solutions raise.

ANNEX I
SUMMARY INTERPRETATION OF INPUT RECEIVED ON QUESTIONNAIRE ON THE CURRENT USAGE OF AUTHENTICATION ACROSS BORDERS IN OECD COUNTRIES

Section I: Examples of Cross-Border Authentication Implementations					
1. Types of authentication method	2. Purpose, context and nature (i.e. closed/open) of application	3. Industry sectors involved	4. Scope of application (i.e. public sector/private sector)	5. Categories of use (B2C, B2B, B2G etc.)	6. Suitability of application to establish evidence of identity
Australia PKI-based.	Patents and customs. Closed community of users utilising multi-use open community certificates.	IP community, importers and exporters.	Public sector initiatives but PKI service providers can be private sector.	B2G and G2B	Rigorous evidence of identity is a component. For customs application, only continuity of identity is required.
Austria PKI-based.	PKI-based citizen card is an open system used by Austrian citizens as well as foreigners for e-government. System supports other national ID cards (e.g. Belgium, Finland, Estonia). Solutions based on hardware tokens (e.g. health) are closed.	E-Government, Health, education and financial.	Citizen cards can be issued by either the public sector or the private sector.	B2B, B2C, G2B, G2G and G2C.	By means of the citizen card the evidence of identity is guaranteed.
Belgium PKI-based.	ID card.	Legal profession and banking.			
Canada Various methods used, including PKI.	PKI-based government online application is available to all citizens. Various other private sector applications available to customers and clients on a "closed" system basis.	E-govt, legal profession, banking.	Offerings by both public and private sector.	Varies according to system but all categories involved.	Applications establish identity and/or privileges.
Czech Republic PKI-based and ID/password based.	E-government is an open system, most authentication applications are or will be intended as closed systems (e.g. banking, payments, health, education, passport system).	Trade, banking.	Public/private partnership.	All categories.	Some applications establish evidence of identity.
Denmark Not aware of any open cross-border PKI solutions.					

DSTI/ICCP/REG(2005)4/FINAL

Section I: Examples of Cross-Border Authentication Implementations (cont'd)					
1. Types of authentication method	2. Purpose, context and nature (i.e. closed/open) of application	3. Industry sectors involved	4. Scope of application (i.e. public sector/private sector)	5. Categories of use (B2C, B2B, B2G etc.)	6. Suitability of application to establish evidence of identity
Finland PKI and TUPAS authentication service (user ID/one-time password).	National ID system is open to all citizens or foreigners permanently residing in Finland. Finnish banks are producing TUPAS authentication service for third parties i.e. for e-service providers. The service provider for which the banks produce TUPAS-service must meet requirements and have an agreement with every bank producing TUPAS service.	Financial services, insurance, trade unions etc.	ID solution offered to both sectors. Banking e-identification used in both sectors as well.	Varies according to system but basically all categories involved.	Systems establish evidence of identity.
France PKI-based.	Health application is a closed system used to authenticate insures and health professionals for payments for services. VAT application is also a closed system (i.e. requires an initial exchange of documents between organisations and the CA).	Healthcare and VAT applications.	Public sector initiated.	G2B, B2C and G2C.	Both systems establish evidence of identity.
Germany PKI and ID/pass-word based.	E-government, and passport systems are suited to cross-border context.	E-government applications are open to all parties involved.	Offerings by private and public sector. The latter procured by public sector through private sector contracts.	All categories.	Improved evidence of identity defined target for passports. All qualified electronic signatures establish evidence of identity.
Italy PKI token-based (smart card).	Open system used for identification (physical world and online), E-government services, health etc. Also used to establish the identity of the originator of an electronic document and to state the signatory's approval of the document signed.	Designed for e-government but can be used in every industry sector.	Public sector-based.	G2C, G2B, G2G, B2C, B2B.	Yes.
Japan No system to collect authentication usage information.	System to authenticate travel documents under development (within ICAO).				
Korea PKI.	E-Trade application is an open system that automates all international trade procedures.	E-government, trade, banking, stock trading.	Schemes operate in both public and private sectors.	All categories.	Applications establish evidence of identity.

Section I: Examples of Cross-Border Authentication Implementations (cont'd)					
1. Types of authentication method	2. Purpose, context and nature (i.e. closed/open) of application	3. Industry sectors involved	4. Scope of application (i.e. public sector/private sector)	5. Categories of use (B2C, B2B, B2G etc.)	6. Suitability of application to establish evidence of identity
Netherlands Various methods used, including PKI.	Most authentication gateways are intended for closed groups (e.g. bank clients, students, etc.). E-govt is an open system.	Banking, education, e-government	Offerings by both public and private sectors.	B2C, G2B, G2G.	The strength of identity depends on the method.
Norway Various. PKI-based and ID/password based.	Closed system for public admin and inspections in aviation sector, public registry functions, chemical industry, and payments.	Aviation, chemical, payments and public sector admin.	Public sector, private sector and joint partnerships.	Varies according to example but basically all categories involved.	Varies but some applications do establish identity.
Slovak Republic PKI.	Open system involving CAs accredited by the National Security Authority.	Crosses industry sectors.	Root CA is a public administration but service providers are private companies.	All categories.	Yes.
United States Varies. Some PKI-based, some token and one-time user passwords.	Example discussed is closed system for communication between government and commercial industry.	Aerospace and Government.	Public/private sector partnership.	G2G, G2B and B2B.	Yes

Section I: Examples of Cross-Border Authentication Implementations			
	7. Degree of, and circumstances for, legal effect of application (domestic)	8. Extent of use of application	9. Existence of privacy enhancing features (e.g. use of multiple identities, pseudonyms)
Australia	Legal effect accorded pursuant to the Electronic Transactions Act.	No data available.	Applications support multiple IDs & pseudonyms. International recognition of digital certificates across diverse national domains.
Austria	Legal effect pursuant to the Austrian Signature Law, EU Signature Directive and the Austrian E-government Act.	4.5 million ATM cards 8 million health insurance cards (eventually 20 million in Europe will have access to the system).	The e-government concept and e – government act foresee derived identifiers in different sectors based on a unique identifier of the citizen card (secure identification with respect to data protection/privacy). The concept is also applicable in the private sector. Cross-border recognition established by the EU Signature Directive, e.g. Belgian, Finnish and Estonian cards already integrated.
Belgium	Legal effect established in legislation.	Too early after launch for data to be available.	Interoperability is facilitated by standardisation of e-signatures.
Canada	Legal effect pursuant to federal legislation in the case of federal government form requirements and provincial legislation in the case of contractual relationships.	400 000 users of government on line services. No data available on private sector usage rates.	Legal and policy complications with arriving at agreements between principals.
Czech Republic	Legal effect established in legislation (e.g. E-signature legislation).	No data available.	
Denmark			
Finland	Legal effect established in legislation.	70 000 ID cards 3.5 million banking customers having banks' user IDs and one-time passwords.	No barriers in financial applications. Variations in implementation of EU Directive means that risks and costs vary for service providers and users. Common standards in software, card readers etc. will lead to better electronic infrastructure.
France		60 million cards issued to the public and 200 000 issued to healthcare professionals. No data for VAT system.	EU project underway for delivery of health services between member states. VAT system can be deployed in a cross-border context.
Germany	Regimes of standards and specs apply.	400 government services to be made available on line involving over 100 authorities.	Standards-based approach means that barriers are largely ruled out.

Section I: Examples of Cross-Border Authentication Implementations (cont'd)			
	7. Degree of, and circumstances for, legal effect of application (domestic)	8. Extent of use of application	9. Existence of privacy enhancing features (e.g. use of multiple identities, pseudonyms)
Italy	Domestic legislation and the European Directive establishes legal effect.	Public sector pilot phase involved 1 million cards. Full deployment to begin next year. In private sector, over 10 million cards issued/used.	Personal data is recorded on the card but is not transmitted through the network. Authentication uses a hash function of personal data and unique identifiers. Pseudonyms are permitted. Lack of inter-operability between applications based on PKI (cert extensions used differently by EU members), need for a common policy for cert and CRL management. There are also legal and cultural differences on signature and authentication value as well as differences on enrolment procedures.
Japan	E-signature legislation establishes legal effect for domestic and foreign signatures.		
Korea	Legal effect established in legislation. Reciprocal recognition of foreign signatures and certs established by agreement.	11 million certificate users in Internet banking, online stock trading, e-government services, online credit payments, etc.	Procedures for cross-certification are complex. Liability is an issue. There is a lack of actual business models to which PKI can be applied.
Netherlands	Legal effect established in legislation.	Only one application (education) has a significant number of users (hundreds of thousands).	In principle no, in practice yes. For example, users must be account holders at certain banks to use the financial application.
Norway	Legal effect established in legislation.		Pseudonyms not supported. Certificate issuance to subjects in foreign countries, establishing relationships with approved CAs in other countries, national confidentiality of certain information.
Slovak Republic	Legal effect established by legislation.	Certification service providers not required to supply this information.	No technical barriers exist but bilateral or multilateral treaties are required for the acceptance of foreign certificates.
United States	Legal effect established in national legislation.	Application is work in progress, no statistics as yet available.	Legal complications could arise from ability of parties to select from a variety of technologies. Recognition of the credentials of others. Establishing legal agreements between principals.

Section II: National Uses of Authentication Technologies		
11. Factors affecting national use of authentication and digital signatures	12. International or transnational legal/institutional frameworks applicable to national implementations	13. Clusters of service providers and extent to which they operate internationally.
Australia Gatekeeper evaluation and interoperability processes ensure CAs and RAs meet government requirements for integrity and trust.	UNCITRAL Model Law on Electronic Commerce.	Australian Government Authentication Framework provides guidance for businesses on how to conduct transactions securely with Australian government agencies.
Austria E-government has motivated the private sector to some extent but low transaction numbers, complexity of technology and lack of understanding of security benefit are inhibitors. In B2B, electronic billing identified in study as potential "killer application". Use of electronic signatures is not mandatory.	EU Signature Directive.	Clusters that exist (as described above), operate only at the national level.
Belgium Use of electronic signatures is not mandatory.	EU Signature Directive.	National applications based on ID card are being developed and tested.
Canada Flexible regulatory framework is conducive to uptake. Technology-neutral approach has caused some uncertainty and hesitancy in the market (due in part to the absence of standards). Users lack information on the benefits of authentication. National tradition of using handwritten signatures. Negative attitude of users with regard to user fees and trust in authentication technologies.	UNCITRAL Model Law on Electronic Commerce. EU Signature Directive.	Financial institutions are the largest group offering authentication (payments and online banking). Payments can be conducted on an international basis.
Denmark Liberal Finnish regulatory framework is fostering the use of various technologies. Implementation of standards and issue. User-friendliness a challenge that needs to be addressed. Fees negatively impact usage rates. Confusion around signature types.	EU Signature Directive.	Banks provide external authentication and TDC (telecom company) provides external authentication based on public requirements defined by the Danish state.
Finland Despite enabling legal framework, few open systems have emerged. Wide use of smart cards has a positive impact on authentication based on such cards. Requirements grid being developed to specify levels of security required for various applications.	EU Signature Directive.	Major banks and telecom operators operate domestically. Finland participating in EU project for use of ID cards across member states.
France Despite enabling legal framework, few open systems have emerged. Wide use of smart cards has a positive impact on authentication based on such cards. Requirements grid being developed to specify levels of security required for various applications.	EU Signature Directive. Ordinance to be developed to correspond with the intersectoral requirements grid (see above).	An industry-wide certification service provider has been created. Can address domestic and European market demands.

Section II: National Uses of Authentication Technologies (cont'd)		
11. Factors affecting national use of authentication and digital signatures	12. International or transnational legal/institutional frameworks applicable to national implementations	13. Clusters of service providers and extent to which they operate internationally.
<p>Germany</p> <p>Legal framework in place. In the past it was considered too complicated by many application providers. Since an Amendment in January 2005, the issuance of certificates for electronic signatures has become much easier. Common standards needed for higher degree of inter-operability (see #13: Signature Alliance). User fees are still an obstacle but expected to decline due to the eCard policy.</p>	<p>EU Signature Directive.</p>	<p>Trust centres, banks, manufacturers and the public administration are represented in Germany's Signature Alliance. The Signature Alliance is developing common criteria based on the profile ISIS-MTT, a composition of international standards.</p>
<p>Italy</p> <p>Fostering factors: high level of standardisation (within Italy inter-operability is assured), complete and mature regulatory framework, effectiveness in healthcare applications.</p> <p>Impeding factors: dependence on smart card reader, few applications based on electronic authentication.</p>	<p>European Directive 1999/93/EC on a Community Framework for Electronic Signatures.</p>	<p>Assocertificatori operating at national level.</p>
<p>Japan</p> <p>Electronic signature legislation is technology neutral and does not regulate or restrict interoperability. Legislation has enabled the use of electronic contracts in B2B transactions.</p>	<p>Electronic signature law is based on the UNCITRAL Model Law on Electronic Signatures.</p>	<p>No group of authentication service providers exists.</p>
<p>Korea</p> <p>Fostering factors: More than 31 million Internet user infrastructure (as of December, 2004), and Internet business such as Internet banking, online stock trading has boomed. Certificates are interoperable between CAs (Certification Authorities). Mandatory certificate usages in the financial sector, such as Internet banking and online stock trading.</p> <p>Impeding factors: Internet content providers are reluctant to deploy certificates due to their sales cut. Complex procedures for certificate issuance and usages.</p>	<p>Domestic legislation reflects the media-neutrality and functional equivalents of the UNCITRAL Model Law on Electronic Signatures.</p>	<p>National PKI (for citizens and corporations) has six accredited CAs.</p>
<p>Netherlands</p> <p>Cost and user-friendliness has inhibited uptake of strong (i.e. PKI-based) authentication. "Light or "middle" authentication is more attractive.</p>	<p>EU Signature Directive.</p>	
<p>Norway</p> <p>Regulatory framework and standards have fostered use. Inter-operability issues, lack of user friendliness and user fees are impeding use.</p>	<p>EU Signature Directive and sectoral legislation.</p>	<p>Banks are collaborating on a PKI-based scheme for eIDs. Public/private sector joint project underway on inter-operability standards.</p>
<p>Slovak Republic</p> <p>Factors impeding use include lack of applications for e-signatures in practice, national tradition of using handwritten signatures and negative attitude towards user fees.</p>	<p>EU Signature Directive.</p>	<p>Private sector certification service providers offer qualified certificates to users for various applications.</p>

Section II: National Uses of Authentication Technologies (cont'd)

11. Factors affecting national use of authentication and digital signatures	12. International or transnational legal/institutional frameworks applicable to national implementations	13. Clusters of service providers and extent to which they operate internationally.
<p>United States Certain types of transactions still require hand signatures. Technology neutral approach leads to lack of standards. Perceived level of user friendliness of PKI and lack of understanding of trust frameworks impede progress. Relaxed regulatory framework has fostered growth.</p>	<p>No.</p>	<p>In many cases, providers are operating at the national level. Financial services operate at the international level. Corporations have emerged in the market as developers and providers of services to the private sector.</p>

ANNEX II
QUESTIONNAIRE ON THE CURRENT USAGE OF AUTHENTICATION ACROSS BORDERS IN
OECD COUNTRIES

Section I: Examples of use of authentication technologies in a cross-border context

Respondents are to provide information on examples of authentication technologies with a focus on cross-border use. Possible criteria for selecting examples of authentication technology applications could be those that are the most successful, most promising or the most widely used. For each of the examples selected, respondents are asked to provide a description of the application/method and its use, which could include, but is not limited to, information on the following aspects:

1. Name the type of authentication method (e.g. PKI, combination of user ID / password, token-based methods). Please explain and provide Web citations (preferably in English and/or French language, as available).
2. What is the application's purpose and the context within which it is used? Is the authentication application/method an "open" or "closed" system? (*Note: For the purposes of this discussion, "closed" involves a prior or existing relationship among the various parties involved in the authentication process.*)
3. Is the authentication application/method specific to a special industry sector? If yes, please specify the sector(s).
4. Is the application/method offered by the:
 - Public sector (e.g. based on a national ID card).
 - Private sector.
5. In which of the following categories is the application/method used?
 - Business-to-business (B2B).
 - Business-to-consumer (B2C).
 - Government-to-business (G2B).
 - Government-to-government (G2G).
 - Government-to-citizen (G2C).
 - Other (please specify).
6. Is the application/method in question suitable for establishing evidence of identity?
7. Is the use of the application considered to have legal effect at the domestic level? If so, please:
 - Reference the legal framework that applies.
 - Describe the circumstances under which the legal effect may be established.
8. Please quantify the application's use (e.g. registered number of users, actual number of usages/year, etc.).
9. Does the application/method support privacy enhancing features, such as multiple identities or the use of pseudonyms? If yes, please provide details.
10. Are there actual or potential barriers to the cross-border use of the application/method from the supplier/user perspective (e.g. legal, technology-related, organisational, trust-related, or other. Barriers may also arise from factors at the national level; see Section II below).

Section II: National uses of authentication technologies

Information is sought about factors that have been identified in OECD member countries as possible incentives or barriers to national uses of authentication technologies and digital signatures, whether linked to technical, economic, or social aspects of the use of such technologies, or to the national regulatory framework.

11. Please describe any factors that have been identified in your country as fostering or impeding the national use of authentication technologies and digital signatures and their evolution over time, *e.g.* with regard to:

- Impact of the regulatory framework.
- Standardisation or the lack of standardisation.
- Interoperability of existing offers.
- User-friendliness/ergonomics of existing offers.
- User fees charged.
- Stability or lack of stability of tariffication models.
- National tradition concerning the (legally prescribed) use of handwritten signatures.
- Attitude of users (*e.g.* cautious uptake of use) and identified background of such attitude.
- Liability of authentication service providers.
- Other (please describe).

12. Is the legal and institutional framework in your country implementing an existing international or transnational framework (*e.g.* European Directive 1999/93/EC on a Community Framework for Electronic Signatures, UNCITRAL Model Law on Electronic Signatures)?

13. Have groups or clusters of service providers emerged in your country (*e.g.* government or local administrations, banks, independent corporations) that develop and provide internal or external authentication services or standards for such services? If so, do such groups or clusters only operate at the national level, or are they also active internationally?