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

OLIS : 03-Feb-1998
Dist. : 05-Feb-1998

Or. Eng.

GENERAL SECRETARIAT
LIAISON AND CO-ORDINATION UNIT
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

SG/EMEF/ICCP(98)1
Unclassified

Emerging Market Economy Forum

OECD EMERGING MARKET ECONOMY FORUM (EMEF)

REPORT OF THE WORKSHOP ON CRYPTOGRAPHY POLICY

OECD, Paris, 9-10 December 1997

The Emerging Market Econmy Forum (EMEF) is a flexible programme destined for non-Member economies engaged in market-oriented policy reform and which policy dialogue is considered of interest to Member countries. The participation of non-Member economies in the various activities of the Forum is on a "variable geometry" basis, according to their relevance to the topic concerned. The Emerging Market Economy Forum is managed by the Centre for Co-operation with Non-Members (CCNM) in co-operation with those Directorates of the Organisation responsible for subject areas under consideration.

The Communiqué of the OECD Council, meeting at Ministerial level in May 1997, welcoming the OECD Cryptography Policy Guidelines (adopted March 1997), called for dialogue with non-Members on this subject. The Committee for Information, Computer and Communications Policy (ICCP) therefore organised this workshop under the auspices of the EMEF programme. The objective of the workshop was to use the OECD Guidelines, together with the OECD's Report on Background and Issues of Cryptography Policy, as the basis for deepening understanding of cryptography policy issues in the increasingly globalised information and communications network and the development of electronic commerce.

61461

Or. Eng.

TABLE OF CONTENTS

**OPENING REMARKS BY MR. KUMIHARU SHIGEHARA,
DEPUTY SECRETARY-GENERAL, OECD**

It is a great honour and a pleasure for me to open this Emerging Market Economy Forum workshop on "Cryptography Policy".

This is a very important workshop. At their meeting in May this year, OECD Ministers welcomed the OECD Cryptography Policy Guidelines as an important contribution to international co-operation in this area and called on the OECD to launch dialogue with non-Members as soon as possible. So this mandate from OECD Ministers brings us all here today.

Many people wonder why the OECD is working in the area of cryptography. Cryptography was first developed as a method for encoding information to conceal secret messages. Historically, it played an important role in military and national security communications, and it was most often used only by governments. But as you all know, cryptography does not just have military applications these days.

With information and communication technologies becoming fundamental driving forces in globalisation, issues of the privacy and security of electronic information have grown in importance. For example, cryptographic applications for ensuring the integrity of data and authentication of messages are important tools for electronic commerce.

The governments of OECD Member countries have recognised the need for an internationally co-ordinated approach to facilitate the smooth development of an efficient information infrastructure. Disparities in policy may create obstacles to the evolution of national and global information and communications networks and hinder the development of international trade. The OECD is playing a role in this regard by developing consensus about specific policy and regulatory issues relating to information and communications networks and technologies.

In early 1996, the OECD initiated a project on cryptography policy by forming an Ad Hoc Group of Experts under the chairmanship of Mr Norman Reaburn from the Australian Attorney-General's Department. This Group was charged with drafting Guidelines for Cryptography Policy, which were adopted as a Recommendation of the OECD Council in March this year. I will not go into any detail on these Guidelines as my colleagues are better placed to discuss them than myself.

I would now like to mention another reason why I am delighted to be here with you today. When I was only appointed Deputy Secretary-General of the OECD in May this year, I was given the very important responsibility of management of OECD's co-operative relations with non-Member economies.

I should emphasise that in the globalising world economy, the OECD's co-operation with non-Members is of fundamental importance for OECD's mission. It is a mutually beneficial process which enables both OECD and non-OECD countries to share their own policy experiences.

And in this context, OECD's Emerging Market Economy Forum is a very important programme for policy dialogue, which is open to all non-Members, according to their relevance to the topic concerned.

So I would like to conclude by wishing you all a lively and productive meeting, and I hope that you will all be able to join me at a reception that I will be hosting this evening, after today's discussions.

Thank you.

AGENDA
OF THE EMEF (EMERGING MARKET ECONOMY FORUM)
WORKSHOP ON CRYPTOGRAPHY POLICY

9 December (Tuesday)

10h00-10h30 OPENING SESSION

- Opening remarks

- Practical arrangements

- Background and overview of the development of the Guidelines for Cryptography Policy

10h30-13h00 SESSION I: Principles

The Guidelines identified eight basic principles for cryptography policy which policy-makers should consider. Each of these principles highlights an important concern, but they are interdependent and governments are urged to implement them as a whole so as to balance the various interests at stake. This session provided an opportunity to facilitate understanding why these issues are important for consideration, as well as to raise potential problems which should be further considered. Each sub-session was led by one or two speakers.

I-1 Trust in cryptographic methods

I-2 Choice of cryptographic methods

I-3 Market-driven development of cryptographic methods

I-4 Standards for cryptographic methods

I-5 Protection of privacy and personal data

I-6 Lawful access

I-7 Liability

I-8 International co-operation

14h30-18h00 SESSION II: National perspectives

Several Member countries have already been developing national policies taking the OECD Guidelines into consideration. A number of countries presented their national perspectives on how they balance the various interests at stake. Both Member and non-Member economies had opportunities to express their views and national situations.

10 December (Wednesday)

10h00-13h00 SESSION II: National perspectives (continuing)

14h30- 17h30 SESSION III: Industry and international perspectives

The private sector is a critical partner in the development of the information infrastructure, and many cryptography technologies and products are developed and supplied by the private sector. Private sector representatives were involved throughout the drafting process to develop the Guidelines for Cryptography Policy. This session first provided an opportunity for all participants to learn about how leading-edge cryptography technology works, as well as perspectives of the private sector on the technical and economic aspects of cryptography.

This session further covered international perspectives on the issues from some international organisations, as well as from Member and non-Member economies.

17h30- 17h45 SESSION IV: Where do we go from here?

Issues related to the certification of public cryptographic keys, digital signatures, and Trusted Third Parties will be examined by the OECD Information Computer and Communications Policy (ICCP) Committee in the year ahead. These issues are also discussed in other international fora including APEC, UNCITRAL and ISO/ETSI. This session reviewed current and planned work in these fora and confirm further co-operation between OECD Member and non-Member economies.

17h45-18h00 CLOSING SESSION

- Brief report by the rapporteur

- Closing statement by the Chair.

SUMMARY REPORT OF THE WORKSHOP

9-10th December 1997

Paris, France

Executive Summary

The workshop, part of the OECD's Emerging Market Economies Forum (EMEF - a vehicle for dialogue between the OECD Member countries and non-Member economies), was held under the aegis of the OECD's Information, Computer and Communications Policy (ICCP) Committee, in Paris on 9-10 December 1997.

The objective of the Workshop was to use the OECD Guidelines on Cryptography Policy, (Ref. [O97/62]), together with the OECD's Report on Background and Issues of Cryptography Policy (Ref. [O97/204]), as a basis for deepening and broadening understanding of cryptography policy issues in the increasingly globalised information and communications networks and the development of electronic commerce.

There were 96 participants at the Workshop. In addition to OECD Member countries, participants were invited from 14 non-Member economies, the European Commission and the private sector**.**

The Workshop was chaired by Mr Magnus Faxén, Ambassador, Ministry of Foreign Affairs of Sweden, and began with an opening statement by Mr Shigehara, OECD Deputy Secretary-General. The Workshop was organised in three main sessions, with Q&A throughout:

- presentations, by experts from Member countries, of the eight basic principles outlined in the OECD Guidelines, which cryptography policy makers are advised to take into consideration;

- presentations of Member and non-Member economies' national cryptography policies;

- introduction of leading edge cryptography technologies and their perspectives by private sector experts.

The workshop provided ample opportunity to hear explanations of the latest national and international positions and situations regarding cryptography developments and to compare them. It also provided an opportunity to learn about many experiences in the use and application of the OECD Guidelines, both the successful developments and the issues yet to be tackled.

A number of conclusions can be drawn from the workshop discussion and exchange of ideas. These include the following main results:

- no major failings in the OECD Guidelines, they represent what can be done at present - however, the policies and approaches of Member countries still differ in the way in which they balance the various guidelines;

- since the OECD took up the cryptography issue at the end of 1995, there is a greater understanding and recognition of the importance of cryptography for authentication, integrity as well as for confidentiality purposes both within the business community and the private citizen;

- there is broad consensus on the importance of introducing digital signatures, with many countries adopting laws to support the application of such signatures;

- finding policy solutions compatible with the encouragement of electronic commerce applications has high priority;

- still, further education and awareness is needed concerning the economic stakes;

- there is a need for a more flexible, coherent and consistent approach with regard to export controls;

- there is a need for a coherent approach to legal access of encryption keys;

- there is great caution among Member governments to discuss international co-operation or alignment of cryptography policies. However, the Workshop, intended principally as a dialogue between Members and non-Members present, demonstrated the need for a fruitful discussion forum even among OECD Members in this fast moving and crucial area, in particular it demonstrated the need for closer collaboration at all levels to ensure that cryptographic policy, schemes and solutions, and supporting management infrastructure can interoperate.

Background

Cryptography is a technological means of providing security for information with respect to its confidentiality and integrity. This technology is critical to the development and use of national and global information and communications networks, and the development of electronic commerce. The widespread use of cryptography has implications for the protection of privacy, business and financial information, as well as for public safety and national security.

The OECD Council adopted the Recommendation concerning Guidelines for Cryptography Policy (see Ref. [O97/62]) in March 1997. These Guidelines are intended to promote the use of cryptography to foster confidence in information infrastructures, to help ensure the safety of data and protection of privacy, to stimulate new applications for electronic commerce, and to promote co-operation among governments. The Recommendation is addressed to decision-makers in both public and private sectors of Member countries. Widespread recognition of the Guidelines is, however desirable and non-Member economies are encouraged to adhere to the Recommendation. At the meeting of the Council at Ministerial Level on 26-27 May 1997, Ministers welcomed the OECD Cryptography Policy Guidelines as

an important contribution to international co-operation in the development of electronic commerce, and called upon the OECD to review developments and to launch dialogue with non-Members as soon as possible.

In view of the development of global information and communications networks and the further need to ensure internationally concerted solutions, it was proposed to begin the dialogue with non-Members by holding a workshop in the framework of the OECD's Emerging Market Economy Forum (EMEF).

Workshop

On 9-10 December 1997 the OECD held an EMEF workshop on cryptography policy in line with the Ministerial mandate expressed above. The purpose of the workshop was to deepen understanding of the range of issues with respect to cryptography policy in the increasingly globalised information and communications networks and the development of electronic commerce. The workshop considered the role of governments and the private sector in both OECD Member and non-Member economies.

The participants included delegates and observers from **18** of the 29 Member countries of the OECD and experts from **12** non-Member economies: Brazil; China; Estonia; Hong Kong, China;, Latvia and Lithuania; Malaysia; Russian Federation; South Africa; Singapore; Chinese Taipei; Thailand; and other representatives (from the European Commission, the Business and Industry Advisory Committee (BIAC), the OECD secretariat, and an independent Rapporteur). Non-Member economies that were invited but could not attend the workshop were India and Israel.

The agenda for the workshop (see page 7-8) addressed:

- The Principles

  The Guidelines identified eight basic principles for cryptography policy which policy-makers should consider. Each of these principles highlights an important concern, but they are interdependent and governments are urged to implement them as a whole so as to balance the various interests at stake.

  This part of the workshop provided an opportunity to facilitate understanding of why these issues are important for consideration, as well as to raise potential problems which should be further considered.

- National Perspectives

  Several Member countries have already been developing national polices taking the OECD Guidelines into consideration. Both Member and non-Member economies presented their national perspectives on how they balance the various interests at stake.

- Industry and International Perspectives

  The private sector is a critical partner in the development of the information infrastructure, and many cryptography technologies and products are developed and supplied by the private sector. Representatives from the industrial sector were involved throughout the drafting process to develop the Guidelines for Cryptography Policy. The presentations of

some of these representatives provided participants an opportunity to learn about how leading-edge cryptography technology works, as well as perspectives of the private sector on the technical and economic aspects of cryptography.

- The Future

  Issues related to the certification of public cryptography keys, digital signatures, and Trusted Third Parties will be examined by the OECD Information Computer and Communications Policy (ICCP) Committee in the year ahead.

Opening Session

The Chair of the workshop, Ambassador Magnus Faxén (Ministry of Foreign Affairs, Sweden), opened the meeting by welcoming delegates and outlined the objectives of the two days of discussion and debate.

Mr Kumiharu Shigehara (OECD Deputy Secretary-General, with responsibility for relations with non-Member economies) recalled the objectives of the EMEF workshops generally and made a number of remarks regarding the rapidly evolving context for cryptography, notably its role in global electronic commerce. He highlighted the need for international consensus and regulatory action with regard to the use and application of cryptography. Cryptography is no longer reserved for military and diplomatic uses -- rather it has come to be used as a matter of course by individuals and enterprises. Countries who intend to be full participants in the "global information society" need to encourage the use of cryptography, and in doing so must address the tensions which arise concerning personal privacy and public safety. The Guidelines on Cryptography Policy offer an important step forward in helping countries avoid incompatible policies while reflecting the diversity of national approaches. They are also important for the future mission of the OECD, with respect to its work on electronic commerce and relations with both Member and non-Member economies.

This was followed with an overview by Ms Hiroko Kamata (OECD/DSTI) on the background, development and importance of the Guidelines. This presentation highlighted the use of cryptography for both confidentiality and integrity, for commercial and government use, and to protect privacy and personal data. The eight principles of the Guidelines formed the basis for taking forward the international dialogue and co-operation in the field of information security.

The session continued with some remarks from Mr Hans Bierschenk (BIAC to the OECD) regarding the role of the Guidelines for global trading and electronic commerce. There is a need for a broad industry and government consensus on a number of issues related to cryptography especially in view of the global context. Over the past year there have been a number of important technical, political and commercial developments in the field of cryptography which need to be addressed at the global level. The business community can work together with the OECD to find a way forward to achieve international harmonisation on the use of and policy for cryptography.

Session on the Principles

This session provided an opportunity to address the significance of the eight basic principles of cryptography policy outlined in the Guidelines and the balance between them, as well as discussing the potential issues and problems which need further consideration. This session was divided into sub-sessions each devoted to one of the principles and each led by one or two speakers.

Trust in Cryptographic Methods

'Cryptography methods should be trustworthy in order to generate confidence in the use of information and communications systems'

Dr Ulrich Sandl (Federal Ministry of Economics, Germany) led the discussion on the principle of trust (see Ref. [RD14]). After addressing what the ideal situation might be in terms of achieving a balance between the needs of lawful access and the need for appropriate levels of strong cryptography, the discussion went on to highlight some of the ways to enhance trust in the marketplace and the infrastructure.

It is important to strengthen the cryptographic market without being overburdened by too much government interference. There is a need to foster international co-operation on an equal footing, creating a global framework which is both transparent and open to cryptographic policy and the appropriate use of cryptography.

There is also a need to consider an appropriate set of cost-effective evaluation methods for assessing the suitability of cryptographic systems.

Choice of Cryptographic Methods

'Users should have a right to choose any cryptographic method subject to applicable law'

The discussion on this principle was led, first by Mr Per Helge Sørensen (Ministry of Research and Information Technology, Denmark) and then by Mr Philippe Dejean (Service Centrale de la Sécurité des Systèmes d'Information, France).

The substance of this principle is that the main way to ensure that users use encryption that meets their needs is that users should have a 'free' choice which cryptographic products and services they use. The choice offered to the user is reasonably broad:

- covering a range of different products (both in hardware and software);
- supporting a range of different applications (e.g. email, Web browsers, home banking)either integrated into the application or as a separate, application independent product ;
- bundled together with other cryptographic services such as public-key certification and/or key management;
- integrated into a number of communication technologies and services.

This range and coverage should result in products and services being available that offer different levels of protection at different costs.

The range of users includes:

- the private user/consumer application of cryptographic products for protecting private email, home banking, Internet shopping;

- businesses and commercial organisations using cryptography for example, to protect company information assets, for secure electronic commerce, for creating virtual private networks over the Internet, for access control;

- government institutions and administrations, for example, to protect citizens personal data.

There are areas of application where a minimum of cryptographic protection will be necessary, for example personal data such as healthcare information or in the case of IPR (Intellectual Property Rights), patents and copyright. However, it is difficult to distinguish a clear boundary between 'free' choice and the marketplace, and the legal framework in which such methods are to be used. Generally cryptographic methods can only realistically be used in some form of legal framework.

It is also important to put cryptography in the broader context of information security solutions which includes the use of non-cryptographic methods. Careful consideration needs to be given to the operational costs related to the management of cryptographic keys.

Some governments may decide to regulate the use of cryptographic methods, and although the Guidelines recognise this, they do not suggest that it be mandatory. Of course if regulation is used it should be in proportion and commensurate with the concept of free choice. The Guidelines indicate that the market must not be overly restricted by government controls. There needs to be a limit to the level of control by governments: sufficient for them to be able to discharge their duties in an appropriate manner but consistent with the concept of free choice. The market needs to be able to judge what is suitable.

Although export controls have always been an available means of controlling cryptographic technologies, the trend seems to be a move toward the concept of mandatory key recovery techniques as a complement to export controls.

Market-Driven Development of Cryptographic Methods

'Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments.'

Mr Masaaki Kobashi (Ministry of International Trade and Industry, Japan) led the discussion on this principle. It was emphasised that the eight principles should be implemented as a whole, especially the first four principles as these are closely interrelated. Trust in cryptographic methods and technologies will be created by a market driven approach. For example, initiatives such as the 'Key Recovery Alliance' may contribute to forge trust in key recovery systems and technologies. This principle of market driven development in an open and competitive environment is one of the fundamental issues for cryptography

and this principle could be strengthened by adding the concept 'freely in the marketplace' to specifically reflect these ideas. The issues of authentication and CAs (Certification Authorities) should be addressed by a market driven approach. Also raising the public awareness about the appropriate use and application of cryptographic methods is very important.

Standards for Cryptographic Methods

'Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.'

Mr Nigel Hickson (Department of Trade and Industry, UK) led the discussion regarding standards for cryptography. It was pointed out that current standards need wider promulgation. There is also a requirement for greater collaboration in the development and adoption of standards, respecting the needs of the market and the demands for interoperability. There are a number of areas that need to be further developed, such as criteria and evaluation methods to test conformity, to what extent there is a need for mandatory conformance, who should do conformity evaluation and a better assessment of the market. It was stressed that the OECD Guidelines provide a good starting point. It was also pointed out that portability, like interoperability, was equally as important to achieve global applications. It was recognised that standards should not just be the domain of the more formal international bodies of ISO, IEC and ITU-T, but that there were important industry developed standards to be considered, for example the SET (Secure Electronic Transactions) protocol specifications.

Protection of Privacy and Personal Data

'The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.'

Ms Heather Black (Industry, Canada) led the discussion in this area. During the development of the Guidelines there was considerable debate on the merits of including a principle covering privacy. On the one hand some had thought that the Guidelines should simply reference the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (see Ref. [O80/58]). On the other hand there were good reasons to strengthen the Cryptography Guidelines by providing more comprehensive advice with regard to the use of cryptography as a tool for protecting personal information.

A global infrastructure to support the use of cryptography places the issues of privacy and human rights in sharp focus. Securing access to keys or to information for purposes of law enforcement, public safety and other lawful purposes, must be balanced against the individual's human rights against intrusion and the right to protection of personal information. Exceptional care must be taken to ensure that policies do not, with the best of intentions and in pursuit of the public good, set up a regime of total surveillance, for example road tolls, e-mail traffic, and payment cards all threaten to shrink the sphere of private life and produce a trail of personal information about individuals.

Also, there are privacy implications where on-line verification of identity is obtained such as in the use of digital signatures based on cryptography. Any infrastructures set up to ensure that an individual is who he says he is must be thorough and secure. This means that the extraction of personal information involving, for example, biometric techniques or physical evidence, is closely monitored and controlled so that further use of this data be strictly limited.

Finally there is a privacy issue related to the transportation of personal cryptographic keys and key material, or escrow of keys, across national borders. The European Data Protection Directive permits transborder data flow only if 'adequate protection' is assured in the receiving state. This issue must receive particular attention in the context of cryptography and is closely related to business and security concerns for the same protection.

In conclusion, those developing cryptographic policies and systems need to pay attention to the individual's privacy rights incorporated in international laws and agreements.

Lawful Access

'National cryptography policies may allow lawful access to plaintext, or cryptographic keys, or encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.'

Discussion on this principle was first led by Mr Thomas Hafen (Federal Department for Public Economic Affairs, Switzerland) and then by Mr Philip Reitinger (Department of Justice, United States). There is clearly a need to achieve a balance between the needs of the individual wishing to use cryptography and those of the law enforcement authorities requiring lawful access to encrypted data.

The first part of the discussion put forward the case for a set of basic criteria for lawful access in order to strengthen international co-operation and harmonisation in this field. Such criteria should cover the effectiveness and efficiency of the process of lawful access: such access should be effective and achieve the intended security goals, it should try to focus on 'target groups', and it should not distinguish between cross border transactions and domestic transactions. Also, lawful access must not discriminate between users of different encryption technology for example, the interoperability between key recovery and non key recovery schemes needs to be assured. This discussion went on to suggest that if key recovery systems cannot be renounced, then they should only be implemented if a number of additional conditions are met (see Ref. [RD 8]). Finally the case was made for two alternatives involving access to stored data: by requiring individuals to assist in the decryption process; or by requiring suspects to hand over the decryption keys (see Ref. [RD 8]).

The second part of this discussion put forward the case for a balance to be struck between the needs of business and consumers and the needs of society as a whole. Such a balance could be achieved by creating and promoting key management systems and infrastructures that provide trustworthy services along with lawful access (e.g. based on 'Trusted Third Parties' or 'TTPs'). To enable encryption to be used for greater privacy and electronic commerce, rapid development of such supporting infrastructures is needed: offering authenticated transactions, robust confidentiality services and key recovery features. Key recovery features should enable users and law enforcement authorities, under proper legal authority, to obtain access to encrypted data. This should address the needs of the user while ensuring that public safety is not placed in jeopardy. The OECD principle on this matter attempts to tackle the conflict and the need to balance the interests of all parties by suggesting that nations should consider the benefits of cryptography, and the costs and benefits of lawful access based restrictions on the use of cryptography and then develop appropriate policy. In addition, further consideration should be given to support user trust and privacy with respect to legitimacy (i.e. lawful access can be obtained only by those who have a right to such access; and the process of access should be auditable), the scope of lawful access and transparency (i.e. making the conditions of lawful access known).

Liability

'Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.'

Discussion of the liability principle was led by Mr Stewart Baker (Steptoe and Johnson). Liability rules will influence the cryptography policy to be adopted. There are many questions and issues to be considered, for example, do the liability rules encourage or discourage the use of cryptography (liability for failure to protect data), do they encourage business to use key recovery techniques (liability for unrecoverable data), do the rules encourage key recovery agents (liability for providing keys to law enforcement agents, this includes enforcement of contracts even against third parties), or do the rules encourage responsible behaviour by law enforcement agencies (liability for misuse of keys)? The liability rules should be clearly defined and understood whether established by contract or legislation or a combination of the two.

International Co-operation

'Governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.'

Mr Göran Axelsson (Agency for Administrative Development, Sweden) led the discussion on the principle of international co-operation. This is a very important aspect of cryptography policy especially in the context of global trading and electronic commerce. Co-operation at all levels of government and industry is required to avoid barriers to trade, in particular if lack of security proves to be a 'show stopper' to global electronic commerce. It is important that suitable key management infrastructure is in place to support secure electronic commerce at the international level.

Other issues to be considered include lawful access across national borders, agreed standards and systems that will interoperate, and national versus global information infrastructures. There is a need to raise awareness of these issues and for the OECD to work towards achieving suitable solutions via closer co-operation between governments, industry and commerce, citizens' groups and the research community.

Session on National Perspectives

Several Member countries have been developing national policies taking the OECD Guidelines into consideration. This session heard presentations from a number of Member and non-Member economies on their national situations. The session also gave an opportunity for participants to express their opinions and views on future developments.

Australia

During the meeting an email message was received from Australia. The message first gave their apologies for not attending, they would have liked to attend but this was not possible. Secondly they announced that on Monday 8th December 1997 the Australian Prime Minister released a package entitled

'Investing For Growth'[1]. As part of this package the Australian Government announced that it would adopt the OECD Guidelines on Cryptography Policy was the basis of policy.

Brazil

Dr Acyr Pitanga Seixas Filho (Centro de Pesquisa s Desenvolvimento para Seguranca das Comunicações) presented an overview of the current situation in Brazil. The Government of Brazil has developed a proposal for a National Policy for Privacy and Security of Information Systems. The document embodies the same principles of the OECD "Recommendation of the Council" concerning "Guidelines for the Security of Information Systems" of November 26-27 1992. Currently, such proposal undergoes technical and political evaluation at the highest level in our administration. The proposed policy also refers to cryptographic security issues. Brazil recognises the importance of the principles established on the document entitled "OECD Recommendation of the Council concerning Guidelines for Cryptographic Policy" of March this year. The proposed Brazilian National Policy establishes that, in most cases, governmental use of cryptography should comply with certified standards or minimum requirements. The trade and use of cryptography by the Brazilian private sector should be free but controlled by State. The document considers cryptography a sensitive and dual-use issue and foresees that matters related to import and export controls of cryptographic products might be regulated by law. Brazil remains very interested in co-operating and continuing discussing issues which will permit the implementation of electronic commerce within a Global Information Infrastructure (GII).

Canada

Ms Heather Black (Industry Canada) gave an overview of the current national situation. The development of electronic commerce is important to Canada and cryptography is seen as an equally important issue for the protection of such commerce. The Canadian Government is considering a legislative framework for the protection of personal data in the private sector, and it is reviewing their policy on cryptography. Canada sees the need to remove any potential barriers to the progress of electronic commerce and it is encouraging the development of interoperable security infrastructures as a step in the right direction. The current Canadian policy on cryptography states that individuals and businesses are free to use encryption products with no restrictions on the use or the need for key backup or deposit. There are no import controls on encryption products in Canada but export permits are required for strong customised encryption products.

With regard to security infrastructure the Canadian Government has been developing a PKI[2] (public-key infrastructure) for federal use. This PKI deals with key management to support both digital signatures and confidentiality.

The Government is currently reviewing what it should do to accelerate the use of cryptography in the private sector, what can be done to meet lawful access needs; to encourage development of private sector cryptographic service providers; and they should be done to position Canada's export industries. It has set up an interdepartmental committee to conduct research and assess the various options taking into account the need for an open and transparent domestic process, and the Government is also conducting ongoing consultations with other nations to ensure an international 'fit'.

[1] See www.dist.gov.au/growth/

[2] Communications Security Establishment, *Government of Canada Public Key Infrastructure White Paper* , Ottawa, May, 1997

China

Mr Xiaodong Yang (China International Electronic Commerce Centre, Ministry of Foreign Trade and Economic Co-operation of China) gave an overview of China's national situation. He emphasised the importance of protecting trade and the need for cryptography to help this process. China currently has a national cryptography commission which is considering the whole issue of cryptographic methods for both confidentiality and integrity purposes. It views the OECD Guidelines and this workshop as a good way forward to promote co-operation and future collaboration. The Chinese Government is also considering the various aspects related to the development and management of CA infrastructure to support the use of cryptography.

Denmark

Mr Per Helge Sørensen (Ministry of Research and Information Technology) provided an overview of the Danish situation. Danish cryptography policy is developed under two premises:

- access to high quality encryption is essential in order to fully exploit the benefits of open networks and for the development of electronic commerce;
- use of encryption can diminish the capacity to fight crime.

Since on the one hand the development of open networks and electronic commerce is expected to be one of the main contributors to economic growth and job creation in the future. On the other hand interception of telecommunications is regarded as a very important means to fight crime.

Denmark sees a need for a balanced approach. It sees electronic commerce as a major driver for electronic development, and it recognises the need for a balanced policy that will support the protection of such commerce whilst providing the capacity to fight crime. The question is whether such a balance can be found and what this might be. Technical solutions are not balanced themselves. The effect of technical solutions depends on how they are used and if they are used at all.

The Danish Government has considered the possible option of regulating the use of cryptography based on the introduction of incentives. It has not found it necessary to regulate the use of cryptography. Currently there is free use of cryptographic technology constrained only by the requirements of the Wassenaar agreement., However the issue of regulation is still open. There are a number of national initiatives underway in Denmark to consider these issues. A report on this discussion is expected shortly.

Estonia

Mr Valdo Praust (State Chancellery, Estonian Information Centre) presented the national situation regarding cryptography policy and regulations in Estonia. In 1992 a cryptography research group was formed to consider various aspects of cryptography including: development of security critical information systems, software and hardware developments, and the security evaluation of existing systems. In June 1996 the Parliament adopted the Personal Data Protection Act which takes into account the main international principles of the protection of personal data. In March 1997 the Data Collections Act was adopted, which regulates the State's data collections/registers management.

Also in April 1997 a Commission was formed to define the necessary legal basis for the use of digital signatures and digital documents, and to draft the necessary legislation. The Commission plans to develop an infrastructure for digital signatures including Trusted Third Parties, time stamp services and authorities (CAs) for issuing certificates. It is planned that the above laws and infrastructure will be in place over the next 1-2 years. In September of 1997, Estonia started to develop its own cryptography policy guidelines. A preliminary version of this policy will be ready for public consultation in early 1998 with final approval planned for later in 1998. This policy takes into account the OECD Guidelines and other relevant initiatives, for example, work from the EU and other European institutions and organisations. The use of cryptography will be free and no escrow systems will be introduced in Estonia.

Finland

Ms Kristiina Pietikainen (Ministry of Transport and Communications) presented the national situation in Finland. Finland has not rushed into any particular approach regarding regulation and policy for cryptography. The Finnish Government is studying developments elsewhere before arriving at some decision as to what course of action to take. It has established a group of experts to see if a law is needed for digital signatures. They envisage that some form of licensing will be required for CAs but it is not known yet whether this will be mandatory or voluntary. There are a number of pilot CA initiatives taking place. A study on data protection is under way which is intended to provide a better understanding of some of the problems and issues to be addressed.

It is their intention of the Finnish Government to keep legislation to a minimum and non-technology specific. There is strong opposition nationally with regard to key escrow/recovery and lawful access. To date the lack of legislation regarding digital signatures has not hindered their use of electronic commerce in Finland.

France

Mr Philippe Dejean (Service Central de la Sécurite des Systèmes d'Information) gave an overview of the situation in France. Before 1986, France had a very strict regime regarding the use of cryptography which meant that it was, in practice, almost banned for the 'layman'. Between 1986 and 1992, the regime changed and cryptographic technology and equipment became declassified although their use was still subject to an authorisation by the Ministry of Telecommunications. In 1992 a specific piece of legislation was enacted which defined the principles and arrangements under which cryptographic technology could be used, supplied and exported. This cited two particular cases for the use of cryptography: (i) that for confidentiality where authorisation is needed and (ii) that for other applications such as integrity and authentication where just a simple declaration is to be made. In 1996 the legislation was changed. The principles of the 1992 Act remained the same, but in addition absolute freedom was introduced for some kinds of encryption equipment or provisions of service, the control of information from countries outside the EU and a deadline for authorisation to be granted. In the 1996 Act:

- **What is unconstrained** is: (i) use of equipment that does not provide for confidentiality, (ii) use of equipment that does provide for confidentiality when keys are managed by a licensed third party, and (iii) use, supply, import and export if included in a list published in an administrative order;

- **What must be declared** is: (i) supply, import and export of equipment that does not provide for confidentiality, and (ii) use, supply, import and export if included in a list published in an administrative order:

- **What must be authorised** is the use, supply, import and export of equipment of everything that does not fall under the previous categories.

The provisions for lawful interception are made in the 1991 Telecommunications Act. This covers two kinds of interception: (i) interceptions authorised by a judge for gathering evidence, and (ii) security interceptions authorised by administrative orders for use in dealing with terrorism, drug smuggling and other severe threats. Seizure of files is a normal part of criminal investigations.

Germany

First, Dr Ulrich Sandl (Federal Ministry of Economics) gave an overview of the national situation in Germany. This was followed by a presentation by Dr Christian Schneider (Utimaco Safeware AG) on the German Digital Signature Act.

Dr Sandl stressed the importance of user protection and the need to achieve a balanced approach in the use and regulation of cryptography. It was suggested that there was too much focus on lawful access and not enough on user requirements. There does not seem to be a convincing argument for bringing together lawful access with the economic requirements/applications. There is certainly a need for greater international harmonisation in the whole area of cryptography.

Dr Sandl went on to give an introduction into the German Digital Signature Law[3] and the Electronic Commerce initiative of the Federal Government (see Ref. [RD 10 & 11]). This overview also provided an introduction to the presentations from industry concerning some of the implementation of certain aspects of the Law. Germany welcomes any international discussion on the Law. The Law was introduced to achieve maximum user protection which is necessary to create trust in the marketplace and the global information infrastructure.

Dr Christian Schneider made a presentation on the implementation of the German Law for digital signatures (see Ref. [RD7]). The presentation provided an overview of the history, objectives and scope, and legal status of the Law. The implementation of the Law involves users, industry, trust centres and a national regulatory body. The technical components involved in the implementation include the means for the creation and loading of signature keys into the system, the signing capability (e.g. using a Smart Card), the secure preparation of the process (signing, verification and secure viewing), a public-key directory and a time-stamping facility. The presentation went on to describe the infrastructure, signing and verification protocols used in the process based on a Smart Card implementation. In conclusion, the development of a digital signature capability with a supporting legal framework provides the way forward for a revolution in the way to do business over the Internet. The number of business transactions over the Internet continues to grow and hence the need for a legally binding, secure means of protecting such transactions.

[3] Germany, *Information and Communications Services Act,* August 1997, http://www.iid.de/rahmen/iukdgebt.html

Finally, an additional room document (see Ref. [RD3]), was provided giving further information on the implementation of the German Digital Signature Law with respect to the topic of Certification Authorities. This provides an indication of the certification hierarchy being implemented: levels of root authority and certification authority. The root authority, (a government agency) provides licenses to private companies to operate as a certification authority (CA), publishes license conditions, provides technical guidelines on products (for users/CAs) and procedures (for CAs), certifies public-keys of licensees, publishes accepted algorithms, periodically checks the CA security and so on. The CA provides on-line verification of certificates, authenticates users, optionally generates public-key pairs and stores them on Smart Cards, optionally provides a time stamping service, and so on. The CAs must observe the German data privacy law, they must use appropriate secure components and controls evaluated to ITSEC (Information Technology Security Evaluation Criteria) assurance levels E2 or E4 (whichever is more appropriate) and they operate as a CA in accordance with a security concept that is implemented correctly and approved (see Ref. [ITSEC]).

Korea

Mr Bong-Ha Rha (Delegation of Korea to the OECD) gave an overview of the national situation in Korea (see Ref. [RD15]). Korea has a number of activities underway related to the use of digital signatures and CAs. It is the intention of the Korean government to issue licenses for CA operations. It sees a need to work on cross-border certification issues, in particular with regard to bilateral agreements. The Government is playing close attention to the developments and activities world wide in this area, and has started to consider a future policy on cryptography.

Malaysia

Ms Swandra Ramachandran (Drafting Division, Attorney General's Chamber) presented the current national situation in Malaysia (See Reg. [RD6]). The Government has made a clear and specific distinction, in their various initiatives, between the use of cryptography for confidentiality purposes as opposed to its use for other purposes, notably integrity. To date Malaysia has not formulated a national cryptography policy for confidentiality. At the moment there are no restrictions on access to cryptographic tools for this purpose, there are no import/export restrictions and there has been no attempt to regulate key recovery or to impose mandatory key recovery on users. However, as Malaysia will at large be a consumer country of encryption products, the move to impose key recovery in exporting countries does give them cause for concern. The Malaysian Government is aware of the issues surrounding encryption for confidentiality and the need to balance the needs of law enforcement agencies against the needs of users in terms of privacy, and it is waiting to see how the OECD, the EU and North America deal with these issues.

Malaysia enacted its Digital Signature Act[4] in 1997 but it is not in force yet pending the preparation of the supporting subsidiary legislation. In developing this Act the Government considered the work carried out in the US, Germany and the UK, as well as the work of UNCITRAL and the OECD. The Act states that a CA may only operate if licensed by the Controller of CAs (a government appointed entity). The drafters of the Act opted for mandatory licensing for several reasons including a way of generating user trust in the CA. They also wanted to ensure that only capable and trustworthy persons became CAs and that they provided a good quality of service.

[4] *Digital Signature Bill 1997*, 1997, http://www..au.malaysia.net/dap/digisign.htm

The Act also deals with the rights, duties and liabilities of users and CAs. The Act provides for the legal effect of digital signatures with regard to:

- recognition of the signature verified by a valid certificate issued by a licensed certification authority;
- recognition that a document signed with a digital signature is as legally binding as a document that is signed by conventional means, that is a hand-written signature, thumb print or other mark;
- recognition that a digital signature is a legally binding signature;
- digitally signed documents are deemed to be a written document and to be an original document for evidentiary purposes.

Netherlands

Mr Edgar R De Lange (Ministry of Transport and Public Works) provided an overview of the situation in the Netherlands. Currently the use of cryptography is free in the Netherlands and the only restrictions are on export control, or more specifically with respect to telecommunications where they have specific provisions regarding interception.

In the framework of the national action plan for the electronic highway they started a national project at the beginning of 1997 on the TTP. This action is based on initiatives such as the EU INFOSEC R&D programme and the work on the OECD Cryptography Policy Guidelines. These activities were the trigger for the start of the project. The aims and goals of the TTP project are to identify the conditions for running TTP and for providing services. An important starting point for the project was that it should take a market driven approach, and it should be based on the idea of self regulation and involve co-operation with users and providers. A substantial part of the project work was carried out by an independent consultancy agency (KMG in the Netherlands). The project is in several phases:

- a project plan was produced and approved by a government steering group established for this reason;
- information on a set of draft conditions was collected by studying literature, external policy documents, including the OECD Guidelines, and through interviews and surveys;
- there was a public call for proposals for TTP projects (announced in their Official Journal) this included a call for the participation of users and potential providers as an assessment/reference group;
- a number of projects have been selected and evaluated by an independent auditing committee (evaluation phase is in the final stages of completion);
- the results of the evaluation and auditing process will be used and go towards a cryptography policy document - this policy document be broadly distributed and will be issued to parliament;

- editorial work on this document has started and it is expected the results will be available by Spring 98 (it is also assumed that they will be available on the WWW in 98).

Some preliminary (but not official) results on the content are:

- the number of conditions seem to be limited;
- it is recognised that different classes of TTP will exist depending on the services they deliver;
- it is not foreseen that there will be a the need for major legislative initiatives - if there should be a need to take legal action it will probably be according to existing legislation adapting present legislation;
- self regulation will be used to process certification and accreditation by market parties - this will be quite similar to the procedures based on the UK Code of Practice (BS 7799).

In Summary the project aims to identify the conditions for the parties involved. It is also an initiative for awareness and stimulating actions for the establishment of TTPs or service providers (e.g. a TTP could just be a CA). Furthermore the project was based on a market driven approach. The project is a growing process for the participants involved.

Specific actions which are expected to be part of the results of the project and will be taken up and implemented separately in the next phase. An example of such an action could be consideration of the status of digital signatures (in this respect they don't expect to make major changes at the moment to the present legislation but perhaps there is a need for refining the legal status of the digital signatures).

Mr Martin Buys (Ministry of Economic Affairs) presented room document RD 5, the 'Joint Statement on the Development of the Internet and the Promotion of Global Electronic Commerce'. The US Secretary of Commerce (William M Daley) and the Minister of Economic Affairs (Hans Wijers) of the Netherlands met in October 1997 to exchange views on the state of the development of the Internet and its applications for electronic commerce. The discussion highlighted the common vision shared by the US and the Netherlands of the potential economic, political and social benefits of the emerging global information infrastructure for the peoples of both countries and of the entire world.

Secretary Daley and Minister Wijers were glad to sign together a joint statement on the development of the Internet and the promotion of global electronic commerce. Specifically they agreed on a number of major points:

- the Internet and the potential for global electronic commerce is a very important engine for the world economic growth in the 21st century;
- to enable the digital economy to flourish, governments must agree to allow electronic commerce, and everything that goes along with it, to be a market driven arena and not a regulated activity;
- regulations, legislation and taxation should be kept to a minimum level

- governments and the private sectors world-wide should enter into a series of understandings that will ensure a predictable global legal and commercial environment for the conduct of business on the Internet.

The governments of the US and the Netherlands agreed to work on a couple of major actions to resolve any issues within this framework. Both governments will continue regular discussions to identify mutual priorities regarding the establishment of a digital marketplace.

Norway

Mr Eivind Jahren (Ministry of National Planning and Co-ordination) presented the current situation in Norway. The Norwegian IT Security Council recently submitted a report to the Ministry of Trade and Industry on the need for cryptography policy in Norway (see Ref. [RD16]) This report highlights the use of cryptography in different areas of society and as well as in public administration, covering: purposes of confidentiality, integrity and authentication, trends in liberalisation of the telecommunications market, EU developments, electronic trade and the Internet, Norwegian projects, and trends in technological developments. The report also covered aspects related to the OECD Guidelines, existing laws and regulations, lawful access, export and import controls. The report identified a number of high priority areas related to cryptography policy: (i) Public Administration, (ii) National Security, (iii) Justice Sector, (iv) Health Sector, (v) Privacy, (vi) Standardisation and Interoperability, and (vii) Trusted Third Party Services.

The policy areas for consideration include: (i) legal acceptance of electronic signatures, (ii) secure money transfers for electronic commerce, (iii) review of regulations with respect to lawful access in situations characterised by heavy use of cryptography (to be addressed when these situations are more clarified), and (iv) existing regulations and agreements on export controls.

The Norwegian IT Security Council considers further elaboration of digital signatures and TTP services to be important. There is a need for separating the issues of digital signatures and TTP services with regard to lawful access. Also there is a need to address the issue of key management, certification services, cross certification and their relationship and arrangements with regard to other countries. Developments, testing and initial service provision in the digital signature and TTP service area should not be slowed down, but should continue in both the public and private sectors.

Russian Federation

Mr Vasilij Sernov (Federal Agency for Government Communication and Information) provided an overview of the situation in the Russian Federation. The Federal Agency for Government Communications and Information (FAGCI) is the Russian agency in charge of information protection. All activities and relations linked with communications are within the responsibility of FAGCI and these are also regulated by FAGCI. The legal instruments which defines the rights of FAGCI as the regulated body are as follows: (i) the Federal Law related to federal institutions in charge of government communications and information, (ii) the Presidents Decree of the 5th April 1997 and the Government Decree of December 1992 on licensing of certain kinds of activities, and (iii) the Government Decree of the 15th April 1994 on the import and export of the technical means of communications.

The regulated activities in the field of communications and information is carried out by FAGCI through a established system of government control, licensing and certification. The policy on exports

and imports is implemented by the FAGCI for the benefit of information security for Russia and thus making goods of bad quality not available on the Russian market. This is being done in the following way:

- imports of foreign technical means are not allowed except for (i) 'hot-lines' for government use, (ii) the technical means for communication between Russian enterprises and their foreign partners between offices or branches of foreign companies and their headquarters beyond the Russian national territory (but they do not have the right of selling these means of communications to other entities and they do not have the right of rendering services in the area of communications);

- exports of Russian made means for communications are realised according to the request of a specific buyer, and the buyer must have a certificate from the Russian authorities for the final user of the product and this must be acknowledged by the authorities of that country in which the buyer is registered.

It was pointed out that Russia wants to provide the technical means of guaranteed quality. They also do not support the proposals of some countries to delete restrictions regarding the lengths and transfer of keys to authorised agencies, national or international. They believe that such an approach will lead to monopolisation to the access of the information on an international scale.

As to the issue regarding organised crime and terrorism, in order not to make the technical means of communication available to them, those issues need to be resolved on the basis of legislation of the countries whose technical means of communications are involved.

They consider that the issues of control are of domestic competence of each country concerned. Russian legislation has modes and functions to deal with violations in the field of information protection which is relevant to Russian firms developing the technical means for communications, and can be used to deal with possible violations of foreign states legislation in the field of information protection.

Singapore

Dr Yeow Meng Chee (National Computer Board) gave a report of activities in Singapore. Their IT2000 Master Plan underpins the concepts of an 'intelligent island', broadband networking and a global information hub. The broadband network (referred to as Singapore 1) will reach every home and business to provide and facilitate electronic commerce. Singapore sees the emergence of electronic commerce as a very important aspect of this concept and to future world trade. Digital signatures and the supporting CA infrastructure will be a core part of this development. In anticipating this situation a CA has been implemented in August 1997 to 'jump start' and encourage the emergence of electronic commerce within Singapore.

Current activities in the area of cryptography include the formulation and review of regulations and legislation for both digital signatures and encryption. With respect to digital signatures a draft electronic transactions bill is being submitted to Cabinet and this is expected to be passed sometime early 1998.

They understand that the control policies on encryption are highly complex having to balance the needs for law enforcement and industry. They are working on these issues and they hope to learn from the experiences of the OECD Member countries in this respect.

International collaboration is also important to Singapore. At the APEC summit in Vancouver in November 1997, Singapore signed a MoU with Canada on IT and telecommunication collaboration. One of the thrusts to this MoU is the harmonisation of electronic commerce policies in both countries. An implementing arrangement to this thrust has been reached which covers the classification of PKI in both countries and the mutual recognition of digital signatures issued or made in both countries.

Spain

Mr Francisco López Crespo (Ministry of Public Administrations) presented the national situation in Spain. Currently there are no regulations in Spain regarding the use of cryptographic methods, digital signatures or CAs, however there are export controls which are implemented with respect to the Wassenaar Agreement. There are some general laws that cover the misuse of technology, for example with respect to the use of electronic media or in the case of electronic crime.

Since there is no written policy in Spain the Government is taking a bottom up approach by considering: (i) changes to existing laws and regulations, and (ii) the implementation of TTPs and digital signatures through a number of operational projects and initiatives involving citizens and the public administration. For example, one initiative involves the association of credit card providers together with the Spanish telephone operator, another initiative involves the Chambers of Commerce, notaries and private companies. The Terms of Reference for this work includes: (i) the OECD Guidelines (now available in Spanish), (ii) national legislative activities (for example in Germany, France, Italy, USA, Canada and the UK), (iii) standardisation work (for example within ISO/IEC JTC1/SC27) and (iv) and the recent EU Recommendation (see Ref. [RD13]).

The Spanish Government expects that in the future CAs will be licensed by the government. Elaboration of the legal aspects and the mandated regulation of CAs is expected in about one year's time. Progress to date in support of this includes: (i) the production of draft regulations which covers the provisioning of certificates and the operations of CAs, and the general rights and obligations of users of these certificates and CAs, and (ii) a pilot project to implement a CA (which expects to offer services to almost all villages in Spain via the National Postal Organisation and includes the provisioning of confidentiality and key recovery services). Future plans include: (i) to extend the trial of the CA to provide services to all three of the Spanish Administrations and to the private sector, and (ii) the establishment of a single, centralised office that will deal with certification issues.

Sweden

Mr Göran Axelsson (Agency for Administrative Development) presented the situation in Sweden (see Ref. [RD1]). The Swedish Cabinet Office is currently preparing a set of guidelines and a policy on encryption and related issues, for example, covering digital signatures, protection of confidentiality and Trusted Third Parties. Sweden is looking to achieve a balanced policy on cryptography taking into account the needs of business and private users, the interests of law enforcement, the requirements to control the diffusion of dual-use products and the interests of national security. The aim of the policy is to promote users' access to strong and secure encryption for both private use and for business and government applications. The policy is to be based on a number of recognised assumptions including:

- the right to use cryptography to protect data in storage and communications;

- there are no restrictions on the import and use of cryptographic products and there are no plans to change this situation;

- export controls of cryptographic products will remain the same;

- the need to support the use of electronic commerce a set of national rules and regulations needs to be developed, including the support for the use of digital signatures and the establishment of CAs;

- the requirement to deposit confidentiality keys and the lawful access to plaintext or deposited keys as a condition for export licenses;

- the need for a voluntary licensing scheme in Sweden for key depositing;

- the need to support law enforcement agencies in the fight against crime by providing lawful access to plaintext or deposited keys;

- national regulations need to be introduced in co-operation with other countries and international developments.

The Swedish cryptography policy will take account of the OECD Guidelines for Cryptography Policy and other international agreements. There is a well recognised need for a legal and organisational infrastructure for the voluntary use of public-key systems and for this to be compatible with an eventual international infrastructure.

Switzerland

Mr Thomas Hafen (Federal Department for Public Economic Affairs) presented an overview of the situation in Switzerland (see Ref. [RD9]). The two principles which Switzerland aims to respect in implementing the OECD Guidelines are:

- **subsidiarity** - the private sector should take the lead with market forces deciding about the use and promotion of encryption technology and the building of trust in such technology, subsequently government regulations should only take place where market forces fail to satisfy the public need, and where government intervention is necessary this should be kept to a minimum and must not lead to undue restrictions on electronic commerce;

- **international co-operation -** encryption technology should be facilitated on a global basis with a supporting legal framework for commercial transactions governed by consistent principles across all borders.

Based on a decree issued by the Federal Council of Security in 1991 and a decision made by the Information Technology Security Committee in June 1997, the Federal Office for Information Technology and Systems (BFI) issued several site security policies and a network security policy. These address the minimum requirements and measures which need to be satisfied by all IT systems. The measure include the use of cryptography. The network security policy involves four phases:

- phase 1 - networked systems and applications are protected by firewalls;

- phase 2 - all transferred data is encrypted on all government wide area networks (WANs);
- phase 3 - the transparent data encryption of the WAN is extended to user workstations;
- phase 4 - end to end security is provided at the application level (e.g. for secure email).

A group led by the BFI is defining a framework for a public-key infrastructure and CAs within the Federal Administration. This group will consider the OECD Guidelines as well as other relevant documents such as the EU Communication 'Ensuring Security and Trust in Electronic Communications'.

Mr Kurt Müller (Gretacoder Data Systems AG) then presented an overview of the Swiss Interbank Transaction Security System (IBASEC) (see Ref. [RD4]). The security requirements in this system include those of message authenticity, non-repudiation of sender and receiver, and message confidentiality. Initially this system will support just the Swiss Interbank Clearing System (SIC) but will be extended to add other services later on. The IBASEC architecture is based on a number of standards such as the UN/EDIFACT formats and public-key/CA specifications.

The architecture is application independent and supports a number of cryptographic algorithms. The goal of IBASEC is to provide a highly flexible security infrastructure that:

- will allow the Swiss banks' future business to grow efficiently and competitively;
- supports a common platform for securing all Swiss interbank applications;
- offers an open, flexible design for future enhancements and developments in cryptography;
- uses a commercial CA to enable future electronic commerce with non-banking partners;
- is based on a concept in agreement with OECD guidelines.

Finally Mr Christian Bösch (Zürich Chamber of Commerce and Digisigna) made a presentation of an infrastructure for public-key certificates for electronic commerce (see Ref. [RD2]). This covered the requirements for the secure authentication of subscribers, the integrity of electronic messages, non-repudiation of origin, digital signature guarantees and the use of cryptography for confidentiality. It also covered the services offered by a TTP with regard to user registration, key generation and certification, and directory functions. The issue related to certification within two different jurisdictions and the interworking was presented, including a solution based on an intermediary CA. In its current state this infrastructure implements certificates for signing and verifying UN/EDIFACT messages and VAT related documents. The next stage of implementation will deal with certificates for Internet applications. In conclusion this key management infrastructure development based of TTPs allows:

- participation in a world-wide electronic market as an authenticated participant;
- proof of evidence to third parties for transmitted electronic documents.

This infrastructure is based on a registration and certification which is compliant with Swiss law.

Chinese Taipei

Mr Chuan-Te Ho (Research, Development and Evaluation Commission) gave a presentation of the situation in Chinese Taipei. The Government is just beginning to develop national policy and laws relating to cryptography. They do not intend at present to introduce specific regulations on cryptography, however they are preparing draft legislation on digital signatures. An interdepartmental task force for drafting this digital signature legislation has just been created and a first version should be available in the first quarter of 1998.

Creating a secure and trustworthy electronic government and electronic commerce environment has been their first priority. A blue print for a national PKI was produced in July 1997. The first commercial use of an electronic government CA is one of the pilot projects for cryptography applications which is scheduled to issue identification certificates to the general public in March 1998. Using these certificates a citizen will be able to conduct paper less on-line transactions e.g. to file income tax returns across the Internet.

The Steering Committee for information development and promotion under the Cabinet has decide, in June 1997, to implement a national multipurpose smart card project. One of the project objectives is to strengthen network access identification environment. The cards incorporate an electronic signature mechanism. The Government released a request for information and in interest in October 1997 to which 23 local and international companies have responded with a submission to the Government. There will be 375 local register offices which act as registration authorities in the future.

The issue of PKI is gathering momentum and each country will probably develop a certification structure. The question is how best to develop the co-operation and recognition between OECD Member countries and APEC on this matter. It is recognised that appropriate agreements will be required for international transactions and the benefits of such mutual recognition could be broadened and multiplied through co-operation between OECD Members and APEC. Early in 1997 APEC set up a task force to review and disseminate information on international trends with respect to PKI. This task force has noted the OECD Cryptography Policy Guidelines and recommends that member economies follow work in this area in conjunction with OECD.

They would like to take the OECD policy guidelines into consideration early on as an essential and integral part of the process of formulating policies relating to cryptography.

Thailand

An overview of the current situation in Thailand was given by Dr Pichet Durongkaveroj (National Science and Technology Development Agency). Thailand has been involved with electronic commerce for some time now and recognises the importance of this form of trading as the way forward for the 21st century (see Ref. [RD6]).

Thailand is currently transforming its telecommunications industry in order to cope with the demands of the fast moving electronic markets that are emerging as well as the international movement. The Telecommunications Master Plan is the centre of actions to keep up with the expansion and modernisation of Thailand's telecommunications infrastructure. Under the Plan, three principle issues will be addressed namely liberalisation, privatisation and regulation. Thailand is also a signatory of the WTO's Basic Telecommunications Agreement. These have directed other initiatives to be undertaken which together will pave the way for international entry to the Thai telecommunications market by the year

2006. The Master Plan is also directing reform of the outdated telecommunications laws as well as establishing the regulatory body, the National Communications Commission (NCC).

Electronic Data Interchange (EDI) is seen as one of the cornerstones of electronic commerce. EDI services have been provided to the public for a number of years in Thailand mostly enabling electronic transactions for wholesale and retail purchasing organisations. The Thailand EDI Council (TEDIC) was established in 1994 to facilitate the standardisation of hardware and software systems used in EDI implements and to create awareness amongst potential users. TEDIC is also an active participant of the Asia EDIFACT Board (ASEB). The provision and use of Internet services is a new and rapidly growing market in Thailand. Although the commercial use of the Internet currently focuses on the advertising aspect, it is expected that a transaction based use will proliferate when public acceptance and security issues have been resolved.

It also recognises the importance of information security and the need to protect electronic commerce using cryptography, for example, for applications such as EFT (electronic funds transfer), document transfers and EDI. The Thai Government currently has no policy on cryptography. There are a number of on-going projects that require the use of cryptography such as the protection of the Government's information network, EDI for Customs applications, Internet services, software banks, copyright protection and data protection. The Government is looking to gain public acceptance and involvement in issues related to the use of and policy for cryptography. As electronic commerce is a global problem, Thailand sees that cryptography is an important and critical factor, that there is a need for a comprehensive framework to support its application and that cryptography policy is required.

United Kingdom

Mr Nigel Hickson (Department of Trade and Industry) gave an overview of the situation in the United Kingdom. In March 1997 the UK Government issued a public consultation paper on 'Licensing of Trusted Third Parties (TTPs) for the Provision of Encryption Services'[5]. This paper detailed proposals for legislation of TTPs resulting from an earlier paper from the UK Government of June 1996 which addressed the provision of encryption services on public networks. The paper covered aspects of cryptography related to the licensing of TTPs, their use for confidentiality and integrity purposes, lawful access with respect to confidentiality, legal recognition of digital signatures, and international aspects.

Public reaction to the paper was mixed. In general most of the responses supported the idea of some form of licensing regime, for example, for consumer protection. Most saw the need for the legal recognition of digital signatures. There was opposition in many responses to linking the licensing of TTPs with the aspects of lawful access. It can be concluded from this consultation exercise that some form of voluntary licensing of TTPs/CAs is needed to support confidentiality and integrity services. There is also a need to address the legislative aspects of digital signatures. In addition, lawful access needs to be treated as a separate issue. He noted that a new policy (reflecting the views of the new Administration) will be announced shortly.

United States

Mr Philip Reitinger (Department of Justice, United States) presented an overview of the situation in the United States. Given the diversity of interests, the US government believes a balance must

[5] http://dtinfo1.dti.gov.uk/pubs/

be struck between the various needs of business, consumers, and society in general. Development of a key management infrastructure that will support these various interests could achieve such a balance. This, together with key recovery features should be able to satisfy the needs of both users and law enforcement authorities.

The US envisions a technology neutral, market driven approach, which uses market incentives to encourage readily available key recovery features in the marketplace. In support of this policy the US government has taken a number of steps:

- there have been various moves regarding the easing of export controls for key recovery (KR) products and a number of entities have been approved to act as key recovery agents;
- the export of a number of non-recovery products of a certain key length has also been permitted on the understanding that exporters make commitments to develop KR products;
- money is also being invested to support application of the policy with the Government - there is the intention to use strong encryption for internal Government communications and communications with the public, and to that end an advisory committee has been convened to develop a federal standard for a Key Management Infrastructure (KMI) to allow for federal purchases of KR products;
- the Government has initiated 10 pilot projects to demonstrate the practicality of KR as a part of a KMI, e.g. the electronic filing of patent applications over the Internet incorporating digital signatures and encryption;
- the Executive Branch of the Government is working with Congress to develop legislation which will promote the development of a KMI in a manner consistent with public safety.

In conclusion, the US Administration supports a voluntary, market driven approach. It also supports the creation of a KMI that supports KR products. This approach is considered to be the best way to balance the various disparate interests at stake.

Industry Perspectives

Representatives from industry gave presentations on the developments in cryptography technology and systems applications. These presentations covered:

The Role of Hardware in Cryptographic Systems

Mr Kurt Müller of Gretacoder Data Systems AG gave a presentation regarding the role of hardware in cryptographic systems, in addition to software components (see Ref. [RD4]). His presentation considered the two different types of component in terms of performance and application requirements for cryptography, for example on the one hand the difference between those applications involving high speed, high volume of data (and thus needing broad bandwidths) compared with simple email messages. There may be other security requirements in addition to secure transmission, such as secure access. Also the total cost (e.g. purchase, integration, management and maintenance) over the life time of the security system needs to be taken into account. Consideration needs to be given to whether security is required end to end or whether a security device is to be shared by many workstations (e.g.

security at the network level). Other factors covered included the speed and throughput, processing requirements, tamper resistance, protocol used, testing procedures and so on. He went on to talk about products and how large and diversified the product market is.

Strong Security for Internet Services

This industry presentation, given by Dr Rainer Rueppel of r[3] Security Engineering, provided an insight into the possibilities of being able to secure Internet services using cryptography (see Ref. [RD19]). This enables a secure Internet based 'Electronic Marketplace' to be established. The solution that was presented is based on the use of the SSL (Secure Sockets Layer) protocol to create an application independent secure channel between trading partners wishing to do business across the Web. This solution provides the capability for confidentiality and integrity of messages or transactions and for verifying the authenticity of end users. The presentation continued to describe how this solution is being used by a Swiss bank to provide secure Internet banking. The overall solution described is based on the use of strong cryptographic mechanisms, is Browser and application independent, and is based on the industry standard SSL.

Public-Key Infrastructure & Smart Cards

This presentation, given by Mr Helmut Jäger of Siemens Nixdorf Information Systems, provided an industrialist's view of cryptography for the emerging Information Society (see Ref.[RD18]). It covered public-key infrastructures (PKIs), encryption, cryptographic based applications and smart card technology. It was pointed out that PKI is a critical element of trust for security aware applications on the Internet such as electronic commerce. PKI provides the necessary basis for key management in an open domain such as the Internet. The presentation went through some of the important issues related to PKI, e.g. global agreement on rules, standards and practices, the certification process and the various cost elements associated with using and providing PKI services. It was stated that there is a Constitutional right within Germany for businesses and the citizen to protect the confidentiality of their information using cryptography, whilst recognising the needs of law enforcement. The presentation went on to illustrate some of the main applications that will require a PKI, such as trusted communications, secure Web technology, and secure electronic commerce. Finally the use of smart cards in cryptographic applications was introduced. In particular, the use of smart cards for authentication (e.g. based on biometric mechanisms), digital signature applications, distribution of encryption keys and in the protection of IPR (Intellectual Property Rights).

European INFOSEC Project 'EAGLE'

This presentation on the EAGLE Project was given by Dr Richard Horne of Racal Research Ltd. The EAGLE Project is one of the INFOSEC ETS projects funded by the European Commission. One of the main goals of the EAGLE Project is to demonstrate a network of TTPs to support secure email based on the JWM[6] or Royal Holloway architecture. The partners of this project come from France, Germany, The Netherlands, Sweden and the UK. This demonstrator is based on a client-server system with a server TTP in each of the five countries involved. This network of client-server systems demonstrates the:

[6] *JMW stands for Jefferies, Mitchel and Walker the authors of the architecture, This scheme is also called the Royal Hollway architecture.*

- signing and encrypting of files for transmission as email attachments;
- verification and decryption of received files;
- generation and certification of integrity keys for users;
- management of confidentiality keys for users;
- ability to provide lawful access to confidentiality keys.

More details of this project are in RD 12.

International Perspectives

The workshop heard two international perspectives. The first dealt with the recent communication COM(97)503 from the European Commission. This covered the issue of ensuring trust in the electronic commerce The second presentation covered the work and projects being carried out under the auspices of UNCITRAL.

COM(97) 503 Ensuring Security and Trust in Electronic Communications

Mr Richard Schlechter of the European Commission provided an overview of the recent Commission communication (see Ref. [RD13] for a more detailed description). Basically the communication covers three areas: digital signatures, confidentiality and electronic commerce, and suggests policy actions at the Member State and the EU level in both the areas of digital signatures and encryption.

In order to stimulate electronic commerce and the competitiveness of industry as well as to facilitate the use of digital signatures across national borders, a common legal framework at the EU level is urgently needed. This framework should include common legal requirements for CAs (minimum requirements for their establishment and operation of CAs and requirements for certificates). This will allow the recognition of certificates between Member States. In addition, the European Union should aim at encouraging Member States to implement appropriate measures to build trust in digital signatures. To achieve as wide as possible acceptance of digital signatures, co-ordinated activities between Member States is required. Also it is recommended that the EU should take part in, or initiate, a dialogue with international organisations such as the OECD, the WTO and the UN, in order to establish common technical standards and mutual recognition of legal regulations.

The EC Treaty and the Treaty of the European Union fully respect the competence of Member States with regard to national security and law enforcement. The Treaty provisions on free circulation do not prevent Member States from establishing domestic regulatory schemes with respect to the use of encryption. However, it is recognised that national restrictions can affect the principles of the free movement of services. Therefore. in order to stimulate the development of electronic commerce in the Internal Market the Commission proposes in this Communication to examine whether these restrictions are appropriate. It is emphasised that it is important to distinguish between digital signature services and encryption services as different rules and considerations apply to these two types of service. Therefore the Commission invites Member States to co-ordinate activities with regard to national restrictions and the

impact on the functioning of the Internal Market and to reflect on the possibility of harmonised national rules at the EU level. Additional measures include:

- adapting the dual-use regulation for the cryptographic products market;
- improving the co-ordination of police forces on a European and international level;
- working towards international agreements between the EU and other countries because of the global dimension of electronic communications and commerce.

Further there is a need for various accompanying measures including support for the interoperability of different encryption and digital signature applications, to support the continuation of Community projects, and support the use of digital signatures and encryption in government administrations.

UNCITRAL Projects

Mr Stewart Baker (Steptoe and Johnson) gave a presentation of the projects that UNCITRAL (United Nations Commission on International Trade Law) is undertaking in the area of electronic commerce and digital signatures. This included the work on the Model Law for Electronic Commerce[7], and the work on CAs and secure electronic signatures.

The Model Law recognises 'electronic signatures', not just "digital signatures" based on asymmetric cryptography. This Law has identified that electronic signatures need to have a level of security appropriate to the circumstances in which they are used.

The work being carried out on CAs and digital signatures began with the Utah-Germany-Malaysia model. Recent discussions have expressed concern about rigidity and technology lock-in, particularly with regard to:

- 'free-range certificates' - regulation versus market mechanisms (e.g., accreditation);
- private uses of digital signature technology;
- recognition of foreign certificates.

Signatures are presumed to be secure and binding based on regulation or accreditation. As regards the liability issues, this is being addressed from a contractual and third party perspective.

As regards foreign CAs, the following aspects are being discussed:

- allow local establishment by foreign CAs?
    - exceptions for national security
- recognition of foreign-issued certificates?

[7] United Nations Commission on International Trade Law, *Model Law on Electronic Commerce*, New York, June 1996, http://www.un.org.at/uncitral/texts/electcom/index.htm

- de jure equivalent to local certificates if level of reliability is substantively equivalent (substantive reliability determined by publication or negotiation);

- de facto enforceable if 'as reliable as is appropriate for the purpose'.

Further discussion regarding the private systems has identified the following aspects:

- recognise party autonomy;
- enforce closed digital signature systems if the contract is 'otherwise enforceable';
- use both private agreements and course of conduct to decide whether signatures are sufficiently reliable to be recognised as de facto binding.

Conclusions

The workshop was successful in that it provided ample opportunity to hear explanations of the latest national and international positions and situations regarding cryptography developments and to compare them: policy, regulation, research, pilots and demonstrators, infrastructure initiatives and international co-operation. It also provided an opportunity to learn about many experiences in the use and application of the OECD Guidelines, both the successful developments and the issues yet to be tackled.

Although there remains some caution among governments to engage in formal debate or negotiation concerning further harmonisation of cryptography policy, the informal nature of the OECD's EMEF setting clearly provided a much needed and much appreciated forum for discussion among Members and non-Members alike. Clearly, the outcome of the workshop, the ideas expressed and the awareness of technology developments and what other countries are doing are likely to provoke keen debate back in national capitals.

A wide range of topics was discussed and there was a vigorous exchange and free flow of ideas, opinions, information and experiences. It was, in addition to hearing from OECD Members, equally interesting and enlightening to hear from the non-Member participants about their experiences and developments, and their thoughts about the future.

There appear to be no major failings in the OECD Guidelines, they represent what can be done at present. However, the policies and approaches of Member countries still differ in the way in which they balance the various principle outlined in the Guidelines, especially so regarding export controls and legal access to keys.

Since the OECD took up the cryptography issue at the end of 1995, there is a greater understanding and recognition of the importance of cryptography for authentication and integrity, as well as for confidentiality purposes both within the business community and the private citizen. There are many encouraging signs that cryptography policy is being addressed at all levels along the lines outlined in the OECD Guidelines.

There is also broad consensus on the importance of digital signatures, with many countries adopting laws to support the application of such signatures and supporting CA infrastructure components and developments. Some countries have such legislation in place and are working on further implementations. Some countries are in a consultation phase and are continuing to study the issues.

The industry representatives played an important role in the workshop by giving participants the chance to hear about recent technology developments and by facilitating better co-operation between industry and government.

Clearly significant progress has been made in a number of areas, and a lot of experiences and information have been exchanged as a result of the cryptography policy work done by the OECD. The following is a summary of some of the things that still need to be dealt with:

- greater co-operation and alignment of solutions to support the use and application of cryptography is clearly needed both at the national and international levels to support the information society, electronic communications and commerce (in fact electronic commerce is recognised as a major driver for boosting the market for cryptography), particularly with regard to:
    - improving delivery of electronic transactions and products;
    - designing better and more secure access to services and networks;
    - enhancing trust and confidence;
    - building trust in TTP/PKI developments and implementations;
    - building trust in the interoperability of systems and services;
    - resolve the regulatory uncertainties;
- more wide spread development of cryptography policy is needed, including;
    - taking into account the need to arrive at a balanced approach with respect to addressing the needs of the various stakeholders
    - achieving a minimum set of interoperable standards;
    - deriving methods for evaluating cryptographic systems and products;
    - adopting a more flexible, coherent and consistent approach to export issues and controls;
    - coherent approach to legal access to encryption keys;
- compatible legal schemes must be achieved, e.g. to support the use and application of digital signatures.

Abbreviations

APEC	Asia-Pacific Economic Community
BIAC	Business and Industry Advisory Committee
CA	Certification Authority
DSTI	Directorate for Science, Technology and Industry
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
EFT	Electronic Funds Transfer
EMEF	Emerging Market Economy Forum
ETS	Electronic Trust Services
EU	European Union
GII	Global Information Infrastructure
ICCP	Information Computer and Communications Policy
IEC	International Electrotechnical Commission
INFOSEC	Security of Telecommunications and Information Systems (European Commission)
ISO	International Organisation for Standardisation
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
JTC1	Joint Technical Committee One
KMI	Key Management Infrastructure
KR	Key Recovery
MoU	Memorandum of Understanding
OECD	Organisation for Economic Co-operation and Development
PKI	Public-Key Infrastructure
RD	Room document

SSL	Secure Sockets Layer
TTP	Trusted Third Parties
UNCITRAL	United Nations Commission on International Trade Law
WTO	World Trade Organisation

REFERENCES

[OECD]

The following OECD documents are available on the Web at :
http://www.oecd.org/dsti/sti/it/index.htm

O80/58 Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Paris, September 1980 [C(80)58/FINAL]

O97/62 Council Recommendation Concerning the Guidelines for Cryptography Policy, Paris, March 1997 [C(97) 62/FINAL]

O97/204 Cryptography Policy: The Guidelines and the Issues (The OECD Cryptography Policy Guidlines and the Reoprt of Backgraound and Issues of Cryptography Policy), Paris, 1997 [OCDE/GD(97)204].

[Room Documents]

The following documents were distributed at the conference. All of the documents except RD 17 are available on the Web at : http://www.oecd.org/dsti/sti/it/index.htm

RD 1 “Cryptography Policy -possible Swedish means of action - a report from the Cabinet Offices’ Reference Group of Cryptography” .... presented by Mr. Axelsson

RD 2 “Electronic Commerce - An Infrastructure for Public Key Certificates” .... presented by Mr. Boesch

RD 3 “Certification Authorities according to the German Digital Signature Law” .... presented by Mr. Kersten

RD 4 “Next Generation Swiss Interbank Transaction Security System (IBASEC)” .... presented by Mr. Mueller

RD 5 “Joint Statement on the Development of the Internet and the Promotion of Global Electronic Commerce” .... presented by Mr. Buys

RD 6 “Electronic Commerce in Thailand” .... presented by Dr. Durongkaveroj

RD 7 “Transportation of the German Law for digital Signature” .... presented by Dr. Schneider

RD 8 “Lawful Access “.... presented by Mr. Hafen

RD 9 “National Presentation Switzerland” .... presented by Mr. Hafen

RD 10 “Federal Act Establishing the General Conditions for Information and Communication Services -Information and Communication Services Act-” .... presented by Mr. Sandl

RD 11 “Electronic Commerce Initiative of the Federal Government” .... presented by Mr. Sandl

RD 12 “The EAGLE TTP Demonstrator” .... presented by Mr. Horne

RD 13 “Communication from the Commission -Ensuring Security and Trust in Electronic Communication Towards an European Framework for Digital Signature and Encryption” .... presented by Mr. Schrechter

RD 14 “The Core Principle of the OECD Guidelines on Cryptography Policy on Trust in Cryptographic Methods” .... presented by Dr. Sandl

RD 15 “Korea’s Plan for Enhancing Information Security” .... presented by Mr. Rha

RD 16 “The Need for a Cryptography Policy in Norway” .... presented by Mr. Jahren

RD 17 “Global Information Networks Ministerial Declaration” .... presented by the participants from Germany

RD 18 “German Industry’s view on Cryptography for the Emerging Information Society” ....presented by Mr. Jäger

RD 19 “Strong Security for Information Services” ....presented by Mr. Rueppel

ITSEC European Union : Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, June 1995

LIST OF PARTICIPANTS

WORKSHOP ON CRYPTOGRAPHY POLICY
ATELIER SUR LA POLITIQUE DE CRYPTOGRAPHIE

9-10 December 1997

Paris

CHAIRMAN ***PRESIDENT***	**Mr Magnus FAXÉN** Ambassador Ministry of Foreign Affairs of Sweden
AUSTRIA ***AUTRICHE***	**Prof. Reinhard POSCH** Institute for Applied Information Processing of the Technical University
BRAZIL ***BRESIL***	**Dr. Acyr Pitanga SEIXAS Filho** Director Centro de Pesquisa e Desenvolvimento para Seguranca das Comunicações
	Dr. Eduardo BARRETO Coordenador-Geral de Pesquisa e Desenvolvimento Centro de Pesquisa e Desenvolvimento para Seguranca das Comunicações
	Mr. Denis FONTES DE SOUZA PINTO Counsellor Embassy of Brazil
CANADA	**Ms. Heather BLACK** Department of Justice Legal Advisor Legal Services Industry Canada
CHINA ***CHINE***	**Mr. YANG Xiaodong** (CIECC) China International Electronic Commerce Centre, (MOFTEC) Ministry of Foreign Trade and Economic Co-operation

CZECH REPUBLIC ***REPUBLIQUE TCHEQUE***	**Mr. Vladimir MACHAN** Office for State Information Systems
	Mr. Petr TESAR Ministry of Interior of the Czech Republic
	Mr. Bohumil DOLEJŠÍ Permanent Delegation of the Czech Republic to the OECD
DENMARK ***DANEMARK***	**Mr. Per Helge SØRENSEN** Special Adviser Ministry of Research and Information Technology
ESTONIA ***ESTONIE***	**Mr. Valdo PRAUST** Security Chief Expert State Chancellery, Estonian Information Centre
	Mr. Ahto BULDAS Research Engineer, Cybernetica Ltd.
FINLAND ***FINLANDE***	**Ms. Hannele IHONEN** Researcher, Ministry of Trade and Industry
	Ms. Kristiina PIETIKAINEN Senior Adviser, Ministry of Transport and Communications
FRANCE	**M. Philippe DEJEAN** Service Central de la Sécurité des Systèmes d'Information
	Mme Annie MARI Direction des Affaires Economiques et Financières Ministère des Affaires Etrangères
	M. Laurent PAILLARD Direction Général des Affaires Politiques et de Sécurité Ministère des Affaires Etrangères
GERMANY ***ALLEMAGNE***	**Dr. Ulrich SANDL** Federal Ministry of Economics
	Mr. Helmut JÄGER Siemens Nixdorf Informationssysteme AG
	Mr. Per KAIJSER Siemens AG

Dr. Heinrich KERSTEN
Debis IT Security Services

Mr. METTE
Deutsche Telekom AG

Mr. METTLER
Federal Chancellery

Mr. RÖVER
Brokat Informationssysteme GmbH

Dr. Christian SCHNEIDER
Utimaco Safeware AG

Mr. Klaus-Dietmar JACOBY
Counsellor, Permanent Delegation of Germany to the OECD

HONG KONG, CHINA
HONG KONG, CHINE

Mr. H.C. PANG
Senior System Manager
Information Technology Services Department

HUNGARY
HONGRIE

Dr. Gyorgy PAPP
Director of Informatics
Prime Minister's Office

ITALY
ITALIE

Mr. Gianni BUONOMO
Counsellor at Law
AIPA -Autorità per l'Informatica

Mr. Luigi GAMBARDELLA
Direzione Affari Generali e Regolamentari, Olivetti

Mr. Stefano LAMBORGHINI
Segretario Generale
AIIP Associazione Italiana Internet Providers

Ms. Alicia MIGNONE
Attachée Scientifique
Délégation d'Italie auprès de l'OCDE

JAPAN
JAPON

Mr. Masaaki KOBASHI
Director, Office of Information Technology Security Policy
Machinery and Information Industries Bureau
Ministry of International Trade and Industry

Mr. Kazuhiro TABUCHI
Assistant Director, Second International Organisations Division
Economic Affairs Bureau, Ministry of Foreign Affairs

Mr. Keiichi KAWAKAMI
First Secretary
Delegation of Japan to the OECD

Mr. Mabito YOSHIDA
First Secretary
Delegation of Japan to the OECD

KOREA
COREE

Mr. Bong-Ha RHA
First Secretary
Delegation of Korea to the OECD

LATVIA
LETTONIE

Mr. Juris VILDERS
Director, Tildes datorprogrammu apgads

LITHUANIA
LITHUANIE

Ms. Violeta STARAITE
Expert in Computer Networks
Lithuanian State Data Protection Inspection

Ms. Gailinta VASKELYTE
Expert in Law
Lithuanian State Data Protection Inspection

Mr. Arturas MICKEVICIUS
State Enterprise Infostruktura

MALAYSIA
MALAYSIE

Ms. LEE Hooi Teck
Manager, IT Security,
MIMOS Berhad Taman Teknologi Malaysia

Ms. Swandra RAMACHANDRAN
Assistant Parliamentary Draftsman
Drafting Division Attorney General's Chambers

NETHERLANDS
PAYS-BAS

Mr. Edgar R. DE LANGE
Senior Security Policy Advisor
Telecommunications and Post Department
Ministry of Transport and Public Works

Mr. Johan van TILBURG
Senior Security Policy Advisor
Telecommunications and Post Department
Ministry of Transport and Public Works

	Mr. Martin BUYS Senior Policy Advisor Ministry of Economic Affairs
NORWAY ***NORVEGE***	**Mr. Eivind JAHREN** Deputy Director General Ministry of National Planning and Co-ordination
	Mr. Kjell W. BERGAN Researcher Headquarters Defence Command Norway /Security
RUSSIAN FEDERATION ***FEDERATION RUSSE***	**Mr. Vasilij SERNOV** First deputy director of Department Federal Agency for Government Communication and Information
	Mr. Sergej BELOV Head of Division Federal Agency for Government Communication and Information
	Mr. Vladimir BAÏKOV Counsellor Embassy of Russia
SINGAPORE ***SINGAPOUR***	**Dr. Yeow Meng CHEE** Head of Security National Computer Board
	Mr. Hoo Ming NG Ministry of Home Affairs
	Mr. Chien Siang YU Ministry of Home Affairs
SOUTH AFRICA ***AFRIQUE DU SUD***	**Ms. Nathalie AFRICA** Counsellor for Multilateral Affairs Embassy of the Republic of South Africa
SPAIN ***ESPAGNE***	**Mr. Francisco LÓPEZ CRESPO** SSITAD Secretary Ministry of Public Administrations
SWEDEN ***SUEDE***	**Mr. Göran AXELSSON** Principal Administrative Officer Swedish Agency for Administrative Development
	Ms. Cecilia HELLNER Counsellor Permanent Delegation of Sweden to the OECD

SWITZERLAND ***SUISSE***	**Mr. Thomas HAFEN** Office fédéral des affaires économiques extérieures Département fédéral des affaires économiques publiques
	Mr. Christian BÖSCH Zürich Chamber of Commerce
	Mr. Robert DIETSCHI Office fédéral de la communication Département fédéral des transports, des communications et de l'énergie
	Mr. Jürg EIHOLZER Crypto AG
	Mr. Kurt H. MÜLLER Gretacoder Data Systems AG
	Mr. Rainer A. RUEPPEL R3 Security Engineering AG
	Mr. Peter TRACHSEL Office fédéral d'informatique Département fédéral des finances
	Mr. Peter PÜNTENER Délégation permanente auprès de l'OCDE
CHINESE TAIPEI ***TAÏPEI CHINOIS***	**Mr. Tai-Yang HWANG** Vice President, Institute for Information Industry
	Mr. Chuan-Te HO Senior System Analyst, Department of Information Management, Research Development and Evaluation Commission, The Executive Yuan
	Mr. Nailiang CHIANG Director, CAPEC
THAILAND ***THAILANDE***	**Dr. Pichet DURONGKAVEROJ** Director of National Information Technology Committee Secretariat National Electronics and Computer Technology Centre National Science and Technology Development Agency
TURKEY ***TURQUIE***	**Mr. Alparslan BABAOGLU** TUBITAK-MAM

	Mr. Mengu BUYUKDAVRAS Minister Counsellor, Ministry of Foreign Affairs
	Dr. Melek D. YÜCEL Assoc. Prof. in EEE Dept. of METU Group Co-ordinator of Information Security in TUBITAK-BILTEN
UNITED KINGDOM ***ROYAUME-UNI***	**Mr. Nigel HICKSON** Head, Information Security Policy Group Department of Trade and Industry
	Dr. Richard HORNE Racal Research Ltd.
	Mr. Tony JERRAM CESG
	Mr. Chris SUNDT ICL
UNITED STATES ***ETATS-UNIS***	**Mr. Philip R. REITINGER** Computer Crime Section, Department of Justice
	Mr. Stewart BAKER Steptoe and Johnson
	Ms. Patricia NUGENT Export Policy Analyst US Department of Commerce Bureau of Expert Administration Office of Strategic Trade & Foreign Policy Controls
EUROPEAN COMMISSION ***COMMISSION EUROPEENNE***	**Mr. Richard SCHLECHTER** DG XIII, European Commission
Business Industry Advisory Committee (BIAC)	**Mr. Hans BIERSCHENK** Fachverband Informationstechnik im VDMA ünd ZVEI (FVIT)
	Mr. Richard BILLSON Corporate Attorney, Microsoft Europe
	Mr. Paul LAMBERT Oracle Corporation
	Mr. Johannes MESSER Program Manager Technical Relations EMEA IBM Germany

Mr. Deniz ERÖCAL
Manager
Business and Industry Advisory Committee to the OECD

RAPPORTEUR

Mr. Ted HUMPHREYS
XiSEC Consultants Ltd.

OECD SECRETARIAT
SECRETARIAT OCDE

Mr. Kumiharu SHIGEHARA
Deputy Secretary-General

Mr. Risaburo NEZU
Director
Directorate for Science, Technology and Industry

Mr. John DRYDEN
Head, Information, Computer and Communications Policy (ICCP) Division
Directorate for Science, Technology and Industry

Ms. Hiroko KAMATA
Principal Administrator
Information, Computer and Communications Policy (ICCP) Division
Directorate for Science, Technology and Industry

Ms. Teresa PETERS
Administrator
Information, Computer and Communications Policy (ICCP) Division
Directorate for Science, Technology and Industry

Ms. Anne CARBLANC
Consultant
Information, Computer and Communications Policy (ICCP) Division
Directorate for Science, Technology and Industry

Ms. Yoko TAKAMA
Consultant
Information, Computer and Communications Policy (ICCP) Division
Directorate for Science, Technology and Industry