



Business and Industry Advisory Committee to the OECD

Comité Consultatif Economique et Industriel Auprès de l'OCDE

BIAC/ICC JOINT DISCUSSION PAPER ON INTERNATIONAL CRYPTOGRAPHY GUIDELINES

May 1996

The Business and Industry Advisory Committee to the OECD (BIAC) and the International Chamber of Commerce (ICC) submit to the Organisation for Economic Co-operation and Development (OECD) this Discussion Paper for OECD discussions on international cryptography policy and the development of OECD guidelines on international cryptography policy.

The sections entitled "discussion points" indicate detailed issues to be discussed jointly by business and government.

I. INTRODUCTION

International business is demanding seamless webs of communications networks whereby information can flow in a free and secure manner. Secure world-wide communications are critically important as intruders, criminals, competitors, and other unauthorised parties find increasingly sophisticated tools to violate the privacy and security of communications. Business needs internationally accepted means for ensuring the confidentiality, integrity, and availability of communications that permit the necessary compatibility of interoperability between different security techniques. Encryption is currently the most appropriate means to ensure security. To ensure security, business needs to be able to use encryption technologies and products (collectively referred to as cryptographic methods) for protection and authentication of its information.

An internationally accepted and comprehensive security policy is essential and needed urgently for business to operate in a global marketplace. There is considerable support for the development of international policies on this subject. Cryptography is mentioned in both the 1980 OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" and the 1992 OECD "Guidelines for the Security of Information Systems" as one of the technological means of assuring protection of personal data and privacy and security of information systems. Specifically, the OECD Security Guidelines state that the "security of information systems is an international issue because information systems ... cross national boundaries" and that governments and the private sector should "consult, coordinate and co-operate ... to encourage implementation of the Guidelines and to harmonise as completely as possible, measures, practices, and procedures for the security of information systems."

ICC and BIAC called for a workable, internationally accepted approach in the May 1994 statement. The urgent need for an internationally accepted approach is widely supported.

II. DEFINITIONS

For the purposes of these Guidelines:

(a) "authenticity" means the property that information comes from the stated source or origin. Message authentication techniques and digital signatures based on cryptography can be used to ensure the integrity of information (i.e., that the information has not been subject to unauthorised changes) and the authenticity of its origin (i.e., that the information comes from the stated source).

(b) "confidentiality" means the characteristic of data and information being disclosed only to authorised persons, entities, and processes at authorised times and in the authorised manner.

(c) "encryption" means the technique by which contents of an electronic message are concealed by a code or a cipher.

(d) "cryptographic methods" means hardware and software techniques, services, and products that use cryptography for the confidentiality, integrity or authenticity of information transferred over telecommunications networks and stored electronically. This includes techniques that do and do not generate keys that can be stored by a key holder.

(e) "encryption key" means a sequence of electronic symbols that determines the transformation from unencrypted plaintext to encrypted ciphertext. For symmetric encryption algorithms, this key can also be used to decrypt the ciphertext to recover the plaintext.

(f) "integrity" means the property that data has not been altered or destroyed in an unauthorised manner.

(g) "key holder" means an entity that holds encryption keys. A key holder could be the owner of the data or a commercial entity independent of the owner of the data (generally known as a trusted third party or an escrow agent).

(h) "trusted third party" means an entity that is trusted by other entities (trustees) with respect to some security-related activity for the purpose of authentication, certification, record keeping, and/or key holding.

III. GENERAL RECOGNITION

It is generally recognised that:

. Cryptography is an important tool to protect the confidentiality, integrity and availability of electronic information, including intellectual and other intangible property.

. There are legitimate commercial, administrative, and individual needs and uses for cryptography.

. Cryptography may occasionally be used by individuals or entities for illegal activities that in turn may affect national security or public safety.

. There is a need for international cooperation on cryptography policy, as incompatible national policies do not meet the needs of owners, users, and governments for globally deployed technologies and applications.

. Policies must strike a balance among the needs of businesses, individuals, public safety and national security.

. Any national or international guidelines and policies must be technology-neutral in terms of product design and development.

IV. GENERAL PRINCIPLES

(1) Free choice

Owners of electronic information have the right and responsibility to protect their electronic information.

It is expected that different cryptographic methods will be needed to adequately fulfil a variety of protection requirements. Users of cryptography should be free to determine the type and level of protection needed for specific information, select cryptographic methods, and implement such methods.

(2) Market Driven

The provision of cryptographic methods should be determined by the market in an open and competitive environment. A market-driven approach to the development and use of cryptographic methods will ensure that solutions keep pace with changing technology, the demands of users, and with the evolving threat environment.

(3) Standards for Cryptographic Methods

Standards for cryptographic methods should be voluntary and international. There may be competing standards. The development of voluntary, international standards should be led by business, with governments' participation.

Standards should include solutions suitable for use by mass market products as well as for business and private use. Suppliers should be allowed to issue suppliers' declarations, certifying that products conform to these standards.

Licenses to intellectual property necessary for compliance with a standard should be made available under reasonable terms and conditions and on a non-discriminatory basis.

Governments should use such products that conform to standards, once available, for all appropriate government purposes, thus instilling confidence in the products' security.

(4) Government Responsibilities and Regulation

Individual Member Countries have the sovereign responsibility to protect public safety and national security. Therefore, cryptography policies should be consistent with national and international law. Additionally, there is a need for international cooperation, as incompatible national policies will not meet the needs of users and their global technologies and applications.

If cryptographic products meet the standards described in Principle 3, these products should not be burdened by any government controls, as long as there are no compelling national security reasons to do so.

Controls imposed by governments for public safety and national security reasons should be clear, publicly available, and to the extent possible, made consistent by international agreement. Governments should process requests under the controls expeditiously and efficiently.

Discussion points:

- Harmonised controls
 - * exceptions from controls
 - * no controls on domestic-use
 - * structure of export controls
 - * periodic review of controls by Member Countries
 - * no controls on products that are routinely and widely available in the global marketplace (foreign availability discussion)
- Length of encryption keys

(5) Key Management

Consistent with the principle of free choice, individuals and commercial entities should be free to choose key management systems. Users will choose key management systems that address their security requirements. Except as noted in Principles 6 and 7, governments should not impose unnecessary regulations on key management systems.

For techniques that generate encryption keys that can be stored, users will choose their key holders. Owners will freely choose the independent entities (for instance a trusted third party) to hold their keys and freely choose to hold their own keys, consistent with any national policy.

Government should not be the sole holder of the key, except for its own internal purposes, or at the discretion of the owner.

Governments should avoid requiring that keys be held within the country as a condition to the importation or use of a cryptographic method. Governments should seek mutual assistance through bilateral and multilateral agreements.

Discussion points:

- Key storage (how long should keys be held?)

- If a trusted third party holds the key, then the key owner and this TTP will have a contract specifying how long to hold the key
- If a government mandates that keys be held longer than the timeframe agreed between the owner and the key holder, the government will incur the cost of doing so. Length of key storage could also be determined
- Compatible laws
- Purpose of keys -- communications vs. storage
- Certification of agents and approval of foreign agents
- Government requirements for the certification or qualification of keyholders should be non-discriminatory and directly related to the key holder's ability to meet key access requirements
- Foreign products that meet government's access needs will be accepted for use in domestic markets

(6) Liability issues

Business is responsible for protection of its information assets and for the cryptographic methods and other techniques that it uses to protect its information. Business cannot be relieved of this responsibility.

Providers and users of encryption methods should agree on the responsibility, accountability and liability for such methods. No provider of cryptographic methods or key holder shall be liable for releasing a key to any lawfully authorised agency of a Member Country.

Discussion points:

- Extent and assignment of liability via contract, or via legislation (domestically or internationally)
- The need for conforming national legislation
- International immunity
- Dispute settlement mechanisms

(7) Government Access

Consistent with national and international laws, governments should have the ability to obtain timely access to encrypted information in plaintext for public safety and national security purposes.

The conditions of government access should be clearly stated, published, consistent with national and international law, and apparent to all users, key holders, and providers of encryption methods.

Government access should be subject to due process of the law. When a government obtains encryption keys for lawfully-authorized decryption purposes, these keys should be used for the authorised purpose only and for a specified time frame.

A government's process for obtaining and using encryption keys should be auditable. These audits must be considered evidence in a court of law subject to due process.

The format of government's requests (for example, a court order) should be easily recognisable by key holders. Key holders that comply with lawfully authorised government requests for keys should be immune from civil or criminal liability.

Discussion points:

- * Governments should discuss the conditions under which they require access.
- * There could be an appendix to these Guidelines that states governments' conditions of access and present laws, including: required level of service in response to requests for keys, the requirement of confidentiality of authorised government access, and if the decryption is limited to specific contents contained in messages.
- * Governments should also discuss specifics of international agreements on access. For instance, there is a need for international cooperation or international agreements between or among governments in cases where the key is requested by a government that is not in the home country of the key holder. These agreements should be publicly available.

(8) International Cooperation

There is a clear and urgent need for international cooperation on all aspects of cryptography policy. Governments should work closely with business to develop and implement harmonised policies to the greatest extent possible. This should apply especially for government controls or regulations placed on cryptographic products, to regulation and certification of key holders, and to conditions of government access.

(9) Implementation of Guidelines

Countries should take any steps necessary to implement these principles in a timely fashion.