



# Recommendations on Authentication in Electronic Commerce

---

May 1999

This document prepared by the Alliance for Global Business (see page 7 about the AGB) is presented to the Joint OECD Private Sector Workshop on Electronic Authentication (Stanford and Menlo Park, 2-4 June 1999), as a minimum checklist of business requirements for government policies addressing authentication in electronic commerce. It contains a brief introduction on the status of authentication technologies and applicable terminology; a set of recommendations addressing government policies and clarifying business action; and suggested actions that business believes the OECD could take to further the market-driven development of authentication solutions to foster electronic commerce.

The recommendations in this document build on the high-level recommendations made by the AGB in its Global Action Plan for Electronic Commerce which was presented at the OECD Ottawa Ministerial Conference in October of 1998. An updated edition of the Global Action Plan will be available in September 1999.

## Introduction

Whether used for providing access to a corporate Intranet or for the identification of communicating or transacting parties (whether commercial or private), authentication techniques play an essential role in electronic commerce. Authentication of the parties to a transaction or communication, when properly carried out by reliable parties and/or through secure technology infrastructures, is a good method of building trust in electronic commerce.

As with all technology, authentication may be implemented at various levels of security and through a number of different technologies based on the requirements of the parties and the transaction or communication. For over twenty years, parties have used passwords and similar methods of authentication in EDI transactions. Today a continuum of technological approaches exists to help facilitate authentication across a variety of business models.

Among the most notable and secure technologies used for authentication are a variety of biometric and cryptographic "key-based" systems used as stand-alones, in combination, or as part of a larger technological solution. Of these technologies, many businesses believe that Public Key Infrastructure (PKI) based tools provide the most scalable solutions for commercially robust authentication available today. While recognising this fact, nothing herein should be read to be a disincentive to the development of new technologies or the application of other technologies which provide appropriate solutions. The following principles should facilitate implementation and deployment of any authenticating technology.

### **Terminology and technology neutrality**

The term "authentication" refers to a large class of electronic applications whose functions may range from pure identification and authorisation to legal recognition. Referring to specific authentication techniques, the terms "electronic signature" and "digital signature" are often used interchangeably. This has led to significant international confusion as to the use of the two terms. "Digital signature" is a functional subset of the more inclusive term "electronic signature". For the purpose of clarity, terminology used in this document shall refer to definitions with a certain level of international acceptance achieved through recognised international fora. The term "electronic signature" has been defined by UNCITRAL as "*a signature in electronic form in, or attached to, or logically associated with, a data message, and used by or on behalf of a person with the intent to identify that person and to indicate that person's approval of the contents of the data message.*" Further, "digital signature" has been defined in ICC's General Usage for International Digitally Ensured Commerce (GUIDEC) as "*a transformation of a message using an asymmetric cryptosystem such that a person having the ensured message and the insurer's public key can accurately determine: (a) whether the transformation was created using the private key that*

*corresponds to the signer's public key, and (b) whether the signed message has been altered since the transformation was made.”*

The distinction between electronic and digital signatures has been at the core of international discussions in recent years on whether policies should focus on electronic signatures or digital signatures. Government frameworks and policies surrounding authentication should facilitate the development and diffusion of existing authentication technologies and business models without disadvantaging emerging technologies. The AGB believes that in legal history there are many examples where different techniques for achieving the same end are facilitated through separate legal frameworks when these techniques reach the stage of commercial viability. It remains essential for governments to ensure non-discrimination. Governments should realise, however, that rulemaking is always limited by the existing terminology and technology to which it will be applied. The AGB believes that governments can and should continue work on an international frameworks supporting the further growth of electronic commerce by promoting a liberal, yet predictable environment in which industry can continue to develop high quality, interoperable, market-driven solutions and standards for certification and authentication.

## Recommendations

### A. Policy principles

Policy approaches to authentication should foster flexibility and diverse business use of technology, practices, and procedures for all authentication tools in electronic commerce. The AGB recommends that such approaches should:

1. Promote freedom of contract

Freedom of contract can include, as appropriate, the following:

- (a) freedom of parties to agree contractually on the acceptance of electronically signed data and to agree contractually on the terms and conditions of transactions (including limitations of liability);
- (b) methodologies for enforcing online contracts and resolving disputes;
- (c) compelling public policy considerations such as public safety and prevention of fraud issues; and,
- (d) use of appropriate terms and conditions through incorporation by reference.

Promoting freedom of contract and maximising available technological and business choices allows parties to craft solutions to meet users' needs while still being supported by appropriate and predictable legal frameworks.

2. Promote technology neutral policies

Technology-neutral policies permit the diffusion of current technologies while not hindering the development of new technologies. Policies concerning authentication should be separate and distinct from policies regarding confidentiality.

3. Address the continuum of authentication systems providing "architectural neutrality"

Policies should not dictate the type of architecture required for authentication. Policies should be architecturally neutral and enable different models to emerge to meet market demands.

4. Promote flexibility as to the content, form and function of certificates or authenticating mechanisms

Policies should be flexible to accommodate the diverse and changing market demands for authentication solutions. In particular, they should allow for certificates and similar devices to provide multiple levels of assurances of identity and/or any other user attributes, as required by market demand. Certificates and other devices used in authentication should conform to appropriate market-driven international standards to help provide commonality and to enable interoperability.

5. Promote free and fair competition

Policies should not discriminate against authentication providers. Policies should promote free and fair competition among authentication service and product providers globally.

6. Enable a predictable international legal framework for authentication

Although at some later stage specific or sectoral rules for authentication may be required, there is an urgent need for generic operating principles for authentication at the international level. There should be market-based, non-discriminatory mechanisms for legal recognition of certificates and similar third party devices providing assurances of identity and/or other user attributes, as well as of the third parties themselves, based on reasonable standards, without necessity of bi-lateral or multi-lateral agreements among independent sovereign states. Any regulatory procedures for recognition of certificates and similar third party devices providing assurances or identity and/or other user attributes should not be written to require local presence/partners or otherwise act as trade barriers. Neutral, objective, commercially reasonable and market-based criteria relating to adequacy should be used to determine recognition.

**B. Business action**

Business will continue to develop self-regulatory frameworks needed for authentication techniques to inter-operate internationally and to allocate equitably responsibilities among various parties to the transaction. Business continues to develop common definitions and best practice guidelines in the authentication and e-commerce arena.

## Conclusion: role of the OECD

We recommend that the OECD could play a strong supporting role in the development of authentication techniques by agreeing to:

- support implementation at the earliest possible time of the UNCITRAL Model Law on Electronic Commerce in all OECD Member States;
- recognise and support the benefits of choice and freedom of contract provided by allowing parties to determine the terms and conditions best suited to their transaction or communication;
- appropriately support the UNCITRAL activity on electronic commerce, including its current work on electronic signatures, certification authorities and related legal issues;
- catalogue, analyse and publicise how OECD Members States implement the 1998 Ottawa Declaration on authentication;

- recognise that mandatory licensing – for commercial and non-governmental transactions - of certification authorities and other third parties providing assurances as to user identity and/or other user attributes will impede rather than benefit the diffusion of electronic commerce across national boundaries;
- promote education and information exchange on the use of market-based mechanisms of recognition, and especially contracts, as a basis of providing for legal effectiveness or validity of messages authenticated using commercially reasonable standards; and
- promote and publicly support development of voluntary, market-based standards and private sector mechanisms for the evaluation of third-party service providers and accreditation criteria and mechanisms.

## About the Alliance for Global Business

The Alliance for Global Business (AGB, "the Alliance") is a co-ordinating mechanism of leading international business organisations created to provide private sector leadership on information society issues and electronic commerce. Jointly, these organisations represent the bulk of electronic commerce in almost all countries in the world. The coalition represents a diverse cross section of business in over 140 countries. Membership includes providers and users of information technology, large multinational enterprises and small start-ups, and companies in developing as well as developed economies.

The founding members of the Alliance are the:

- Business and Industry Advisory Committee to the OECD (BIAC)
- Global Information Infrastructure Commission (GIIC)
- International Chamber of Commerce (ICC)
- International Telecommunications Users Group (INTUG), and
- World Information Technology and Services Alliance (WITSA).

The Alliance has issued a set of fundamental principles as the basis for policymaking for electronic commerce. *The Global Action Plan for Electronic Commerce*, a living and evolving document, calls for minimal government regulation and emphasises business self-regulation as the most effective way of building confidence in transactions over open networks. The initial version of the plan was officially submitted to the OECD governments at the October 1998 OECD Ministerial Conference on Electronic Commerce. It sets out industry's views on the full range of e-commerce issues, including privacy, cryptography, consumer protection in the online environment, taxation of e-commerce, intellectual property protection, standards, competition and Internet governance.

The AGB Global Action Plan describes in detail business initiatives in all these fields so that governments are informed of the extent to which self-regulation is already operating and what further initiatives are under development. The plan's stated aim is to create trust in e-commerce across the whole spectrum of providers of services and goods.

In addition to describing specific business actions and commitments in the field of e-commerce, the plan identifies business expectations in regard to government action. Business would like to see governments concentrate on providing a minimalist and predictable legal framework in specific areas of government competence such as intellectual property protection, taxation, and the removal of barriers to competition in providing the underlying infrastructure. An annex to the action plan contained summaries of various business initiatives. Business executives who compiled the document said these provided ample evidence that comprehensive business self-regulation of electronic commerce is well on its way. The respective roles of government and business responsibilities need to be clarified, and that is what the action plan sets out to achieve. Furthermore, international organisations must ensure that their initiatives do not duplicate or contradict each other.

The Global Action Plan will be used by the Alliance to convey industry's views on electronic commerce in several fora in addition to the Organisation of Economic Co-operation and Development. The coalition has issued a special adaptation of its Global Action Plan entitled "Trade-Related Issues in Electronic Commerce", which is being used in discussions with several other international organisations including the World Trade Organisation, the Asia Pacific Economic Co-operation (APEC) forum, the European Union, the Free Trade Area of the Americas, and others.

## **BIAC – Business and Industry Advisory Committee to the OECD**

The Business and Industry Advisory Committee to the OECD (BIAC) is the voice of business from the economically advanced democratic nations of the world. Recognised by the OECD since 1962 as its business advisory counterpart, BIAC has the mission of ensuring that the OECD hears a broad-based, considered business advice on all sectors of activity that it embarks upon. BIAC's membership consists of the principal industrial and employers' organisations of the OECD Member countries. These represent the majority in terms of employment, output, assets and investment by the private sector in the advanced market economies. Over the years BIAC, its member organisations, and their member companies have been deeply involved in the work of OECD on information and communications and electronic commerce, through direct participation in OECD committees as observer and by providing technical and policy advice to various processes that develop OECD instruments such as the 1980 "Privacy Guidelines" or more recent work on cryptography policy.

## **GIIC - Forum for the Global Information Infrastructure**

Launched in 1995, the Forum for the Global Information Infrastructure (GIIC) is a private sector advocacy group bringing together 50+ CEOs and Presidents of major international corporations with a stake in the development of the GII. GIIC members are from both developed and developing countries. The GIIC serves as a bridge between diverse players and business communities around the world, thus fostering the global dialogue necessary to address critical issues in building the global information infrastructure. The GIIC has established on-going policy dialogues with governments and international organisations, providing them with pragmatic advice and input as they transition to the new body of policies and laws needed to support a secure, seamless global communications environment and marketplace. Four main thrusts of GIIC activity are: 1) facilitating the creation of harmonised rules to support global electronic commerce; 2) bringing developing countries into the process of building the global information economy; 3) spurring the reform of education systems to prepare for the Information Age; and 4) fostering an open environment for the development of information infrastructure and services. GIIC membership is representative of all the major elements of the information technology sector, including telecommunications hardware and services providers, computer hardware and software companies, cable, broadcast, and publishing companies, new satellite companies, international organisations, governments, and academics. The GIIC's regional co-chairs are H. Brian Thompson, (chairman and CEO of Universal Telecommunications), Volker Jung, (executive vice president, member of the managing board, Siemens), and Michio Naruto (vice chairman, Fujitsu). W. Bowman Cutter (managing director of E.M. Warburg Pincus) acts as the GIIC managing director.

## **ICC - International Chamber of Commerce**

ICC is the world business organization. With corporate and business organisation membership in more than 130 countries, it is the only representative body that speaks with authority on behalf of enterprises from all sectors in every part of the world. Founded in 1919, ICC's purpose is to promote an open international trade and investment system and the market economy world-wide. Its rules for international trade transactions and trade finance are accepted globally by traders, governments and judges. The ICC International Court of Arbitration is the world's leading institution of its kind. ICC brings together executives and experts from all sectors of business to

establish the business stance on broad issues of trade and investment policy as well as on vital technical or legal subjects. The ICC's broad framework of rules for international trade and commerce evolves continuously to take into account changes in business practice. ICC has issued best practice rules for electronic commerce since the 1980s and continues to harmonise business rules and practices to meet the needs of the information society.

### **INTUG - International Telecommunication Users Group**

INTUG is an international association of users of communications technology and applications. It has an extremely wide constituency. Founded in 1974, it has its Secretariat in Brussels where it is registered as an international non-profit organisation. It meets in plenary session four times a year. Members include national users groups which represent the interests of users in Europe, the Americas, Asia-Pacific and Africa. Associate and individual members come from major multinational enterprises, academia, law and other relevant industry sectors. Many of INTUG's member groups have been particularly successful in their interaction with national government policy makers; also in regional economic policy forums. INTUG itself promotes the interests of all users at the international level and ensures that the voice of the user is clearly heard whenever communications policy issues are addressed. Its Special Interest Group on Y2K issues has been extremely active and was a specific focus of the INTUG meeting in Brussels in June 1998.

### **WITSA - World Information Technology and Services Alliance**

The World Information Technology and Services Alliance (WITSA) is a consortium of information technology industry associations from economies around the world. Serving as the global voice of the information technology industry, WITSA is dedicated to:

- advocating policies that advance the industry's growth and development;
- facilitating international trade and investment in information technology products and services; and
- providing members with a vast network of contacts in nearly every geographic region of the world.

WITSA:

- serves as a forum for the identification of common issues and views;
- formulates positions on information technology issues, including the recently concluded World Trade Organisation (WTO) Agreement on Basic Telecommunications Services;
- voices the concerns of the international information technology community at multilateral organisations including the WTO, the World Intellectual Property Organisation (WIPO), the G-7 and other international fora where policies affecting industry interests are developed;
- provides information on international marketing and business development;
- promotes information sharing on information technology policy developments throughout the world; and
- hosts the biannual World Congress on Information Technology.