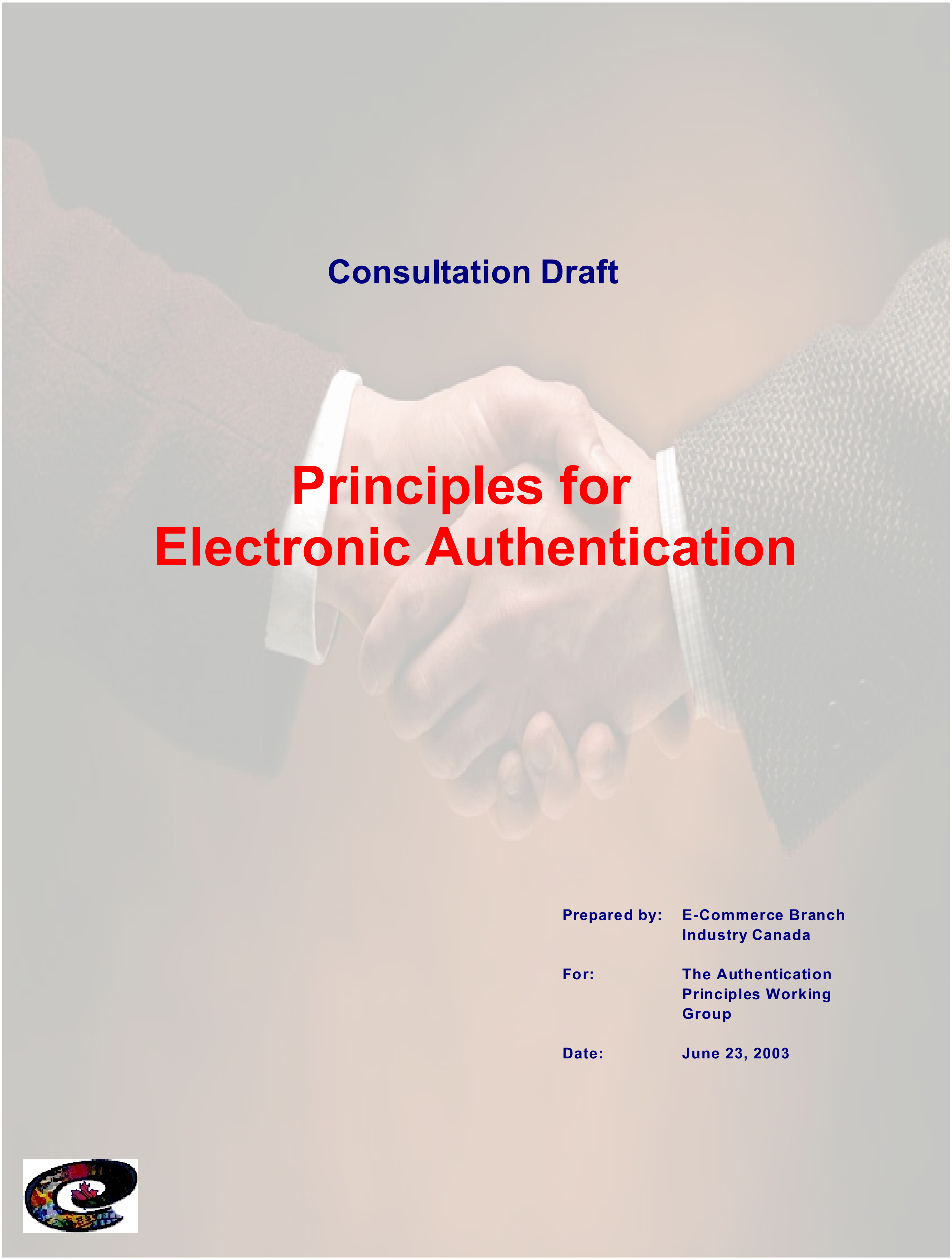

Consultation Draft

Principles for Electronic Authentication

Prepared by:	E-Commerce Branch Industry Canada
For:	The Authentication Principles Working Group
Date:	June 23, 2003

TABLE OF CONTENTS

Part A: Introduction

Background

All Canadians - individuals, businesses, and governments - share an interest in ensuring that electronic communications are secure. As our use of public electronic networks continues to evolve from searching the Internet for information to the exchange of information or money, we need greater assurance that these messages and transactions are secure and that our privacy is protected. Authentication can make a significant contribution to meeting this need and to building user confidence.

> *Authentication is a process that attests to the attributes of participants in an electronic communication or to the integrity of the communication.*

These Principles are designed to function as benchmarks for the development, provision and use of authentication services in Canada. They are intended to form the basis of codes of conduct, voluntary initiatives and guidelines that are tailored to the requirements of specific industry and government sectors. For individual and business users of authentication services, the Principles are intended to be a useful source of information and a benchmark against which to evaluate services offered in the marketplace.

These Principles were developed by a working group, convened by Industry Canada and drawn broadly from industry, professional associations, consumer groups and various levels of government. The following individuals participated on the Working Group:

Bell Canada	David Masse, Senior Legal Counsel
Canadian Advisory Committee, IT Security	Alice Sturgeon, Chair
Canadian Bankers Association	Gary Ferris, Advisor, Banking Operations
Canadian Bar Association	Mairi MacDonald
Canadian Institute of Chartered Accountants	Bryan Walker, Principal, Innovations Group
Canadian Payments Association	Michaela McBean, Senior Officer, Payment Services
CataAlliance	Dave Paterson, Executive Director
Certified General Accountants Association of Canada	Bruce Hutton, Vice-President, CGA Ontario
Deloitte & Touche LLP Canada	Jane Dargie, Senior Consultant, Secure e-Business
	Richard Kitney, Director, Secure E-Business
Digital Discretion Inc.	Stephanie Perrin, President
Fidelity Investments	Heleen Krzycki, Director, Business Solutions
Finance Canada	Andrew Rector, Financial Sector Division
Gowling Lafleur Henderson LLP	Michael Power
Industry Canada (Electronic Commerce Branch)	Peter Ferguson, Director, Policy Development
	Jane Hamilton, Senior Policy Advisor
Industry Canada (Office of Consumer Affairs)	Susan Gardiner, Senior Policy Analyst
Information Technology Association of Canada	Bill Munson, Executive Director, Policy and Planning
Insurance Bureau of Canada	Randy Bundus, General Counsel and Corporate Secretary
	Ron Bilyk, Compliance Officer, Zurich North America
Juricert	Ron Usher, Vice President
Province of British Columbia	Brent Grover, Senior Advisor, Management Services
Province of Ontario	John Gregory, General Counsel, Policy Branch, Attorney General
Public Interest Advocacy Centre	Philippa Lawson, Senior Counsel
RBC Financial Group	David Braidwood, Senior Manager, Standards and Security
	Rosemarie Gage, Senior Manager, eTransactions Policy
Retail Council of Canada	Ken Morrison
Scotiabank	Phil Griffiths, Vice President
Standards Council of Canada	Begonia Lojk, Manager Standards Programs
Spyrus Inc.	Alice Sturgeon, System Policy Architect
Teranet Inc.	Nancy Peng, Product Manager, Security Services
Treasury Board Secretariat	Susan Bryant, Director, PKI Secretariat
University of Ottawa (Law School)	Greg Hagen
Visa Canada Association	Susan MacKeown, Director, e-VISA Canada

The Working Group has achieved consensus that this version of the Principles should be circulated for broader stakeholder review to help ensure that the Principles reflect the broadest possible range of views and interests.

1. Terminology and Concepts

The Principles concern authentication in its broadest sense, taking into account policy, legal and technical considerations. Therefore the terms used are inclusive of the participants, actions and techniques that relate to all aspects of authentication, whether considered from the technical, legal or business perspective.

The defined concepts reflect the Canadian environment. These concepts are all components of authentication in its broadest sense; each concept relates to the others and none should be considered in isolation.

Authentication: *A process that attests to the attributes of participants in an electronic communication or to the integrity of the communication.*

Comment: Electronic *authentication* is used to promote trust in electronic activity. Participants are provided with assurance that other participants in an electronic communication have been authenticated using technological methods and that those other participants, as well as the integrity of the communication itself, can be trusted to the degree specified by the authenticator. The technological methods and specifications used are often based on cryptographic techniques.

Electronic communication: *An electronic transmission, message or transaction.*

Comment: Participants rely on the authentication of an electronic communication to the extent that they can assess the reliability of the authentication.

Attributes: *Information concerning the identity, privileges or rights of a participant or other authenticated entity.*

Comment: The act of authentication depends on some prior activity that authorizes participants, based on their presentation of certain specified *attributes*, to enter into an authenticated electronic communication. The attributes may be inherent, such as identity, or assigned, such as a privilege to enter into a given transaction. Authorization is the responsibility of a designated authority. Many models are available for carrying out such authorization. For example, a simple exchange of information may require as authorization only the presentation of user identification and password. An electronic system established to communicate highly confidential and private information may, by contrast, require in-person presentation of two or more pieces of reliable identification combined with unique personal characteristics, such as fingerprints. Yet another model designates an employer as the authority, who then authorizes a group of employees to engage in electronic communications on its behalf on the basis of the individuals' job functions.

A participant's attributes may relate to a person's identity. As an alternative, the required attributes may identify the person's rights or privileges to enter into the electronic communication. In the latter case, a participant may not need to be identified personally to other participants.

Participant: *An individual or organization participating in an authentication process, whether directly or through another authenticated entity such as a data service or object, hardware device or software program.*

Comment: Authentication processes frequently attest to the attributes of non-human entities. For example, an organization participating in an authentication process may choose to authenticate a server. In this case, the server's attributes may relate to the privileges it has been assigned to communicate with other servers or clients on the system.

Authenticator: *The designated authority that confirms the attributes of a participant or entity and then attests to them to other participants in the electronic communication.*

Integrity: *Assurance that the information in an electronic communication has not been modified or corrupted during the process of communication.*

Note: A term that is not defined or used in connection with these Principles is "non-repudiation". The term is commonly used to describe a technical standard to be met by an authentication process. However, the term is misleading in a more general context because it incorrectly implies a necessary conclusion of law.

2. Functions

For the purposes of these Principles, the authentication process is viewed as encompassing six basic functions. Their relative importance will depend on the purpose and structure of the authentication process. These fundamental functions can be described as follows:

Authentication administration
Administering the measure or measures designed to confirm the attributes of a participant and those designed to support the credibility of a participant's claim to possess those attributes and thereby be authenticated.

Specification
Establishing or selecting an authentication process and delivery mechanism.

End use
Originating or receiving an authenticated electronic communication and relying on the authentication of the attributes.

Standards development
Establishing standards that support the continued development of processes designed to facilitate authentication of electronic communications.

Compliance assessment
Observing and making informed evaluations of the practices associated with authentication to ensure that appropriate policies, procedures and standards are being followed.

Infrastructure provision
Providing the technical capability that enables authentication, including functions to authenticate identity or the integrity of electronic communications or providing the underlying technology used to communicate electronically.

3. Why and How to Use These Principles

The Principles are intended to provide guidance for the development, implementation and use of authentication products and services in Canada. They complement the existing governance structure[1] for authentication by establishing a benchmark to ensure that authentication products and services embody sound business and market practices, meet the needs of Canadians and are accepted internationally.

The governance structure that applies to authentication services in Canada today consists of, among other instruments, relevant federal and provincial legislation including the 2000 *Personal Information Protection and Electronic Documents Act*; the Government of Canada's 1998 Cryptography Policy; the Principles of Consumer Protection for Electronic Commerce, developed in 2001 and the Canadian Code of Practice for Consumer Protection in Electronic Commerce which was approved in principle in January 2003.

It is anticipated that the Principles will be of greatest use to those involved in the design, development and deployment of authentication services and products. The Principles identify the functions and responsibilities of participants in authentication processes and provide a framework to assess and manage the risks that accompany these responsibilities. They also identify security, privacy, disclosure and complaint handling matters which need to be taken into account at each stage of the design, development, implementation, and evaluation of an authentication process.

Those involved with the design, implementation and ongoing operation of authentication processes are encouraged not only to respect the Principles, but also to publicize them. The Principles should form the basis of codes of conduct, voluntary initiatives and guidelines that are tailored to the requirements of specific industry and government sectors. Such sectoral initiatives are strongly encouraged, and can provide strategic advantages in domestic and international markets.

The Principles are intended as a useful source of information and as a benchmark for individual and business users of authentication. Additional legislative or other measures may evolve to address the needs of end users, particularly the risk and liability assumed by individuals participating in authentication processes.

The authentication environment is dynamic and the technologies used will continue to evolve. Although every effort has been made to define Principles that can encompass foreseeable developments, they are open to revision as needed to take into account significant technology advances, changes in market characteristics and international developments. Comments and views on these Principles are welcome at any time and should be addressed to:

Richard Simpson
Director General
Electronic Commerce Branch
Industry Canada
300 Slater Street, Room D2090
Ottawa, Ontario
K1A 0C8

Comments can also be provided by facsimile at (613) 941-0178 or by electronic mail at authen@ic.gc.ca.

The Principles will be reviewed at least every five years, and can be revisited more frequently if necessary. The Authentication Principles Working Group is charged with the periodic review and revision of the Principles. The composition of the Group will be assessed and adjusted as appropriate as the authentication environment evolves.

[1] We use "governance structure" to mean the range of policy tools, regulatory instruments and self-regulatory guidelines that relate to the development and implementation of authentication services in Canada.

4. Scope and Nature

These Principles relate to electronic authentication in its broadest sense.

The Principles are intended to apply to authentication processes used in connection with electronic communications that take place between businesses or governments and other such organizations (known as B to B transactions), between such organizations and individuals as consumers and citizens (B to C), and between consumers or citizens (C to C).

A range of relationships can exist between authenticators and end users, and among end users. Many of these relationships will be governed by an agreement. The Principles are intended to guide the development of these agreements and to apply to the full range of these relationships.

Parties to negotiated contracts are usually best able to determine which terms and conditions suit their particular needs. However, in situations where a party may not have the opportunity to negotiate the terms of their interaction with the other party (or parties) to the transaction, the Principles are of particular importance.

The Principles should be considered and applied as a unified whole.

The provisions in the various Principles are interrelated and interdependent; they cannot achieve their purposes if they are implemented selectively, although not all Principles may apply in all cases. Those applying the Principles to define or implement authentication processes are encouraged to exceed the benchmark established by these Principles and expand upon them to address the requirements of their particular security environment or application.

The Principles are expressed at a high level of generality and technological neutrality.

Canadians can choose from a variety of technologies to authenticate their electronic communications according to the nature of the particular communication and the requirements of the participants.

The implementation of authentication processes will also differ depending on the business or legal objectives to be met, as well as characteristics of the environment in which the electronic communication takes place, such as security and privacy needs and other legislative or regulatory obligations. These factors will define the functionality required of an authentication process and, in some cases, even the type of authentication used.

The Principles are designed to foster a well-functioning, fair and competitive marketplace for authentication products and services.

These Principles reflect the interests of business and governments and take into account consumer input. Wherever possible, the Principles accommodate choice: choice of technology, choice of services, solutions and degree of reliance by end users, and choice of tools used to ensure compliance.

The Principles emphasize proportionality.

The degree of responsibility and risk that each participant in the authentication process assumes should be in proportion to the degree of knowledge and control that the participant can reasonably be expected to have and to exercise, as well as the nature and value of the electronic communication itself. As participants can perform multiple functions in varying combinations, the degree of responsibility and risk assumed by any one participant may vary, depending on these functions.

The Principles emphasize data privacy.

The Principles recognize the existing and evolving legal framework for the protection of the privacy of personal information in Canada, and address how privacy protection standards apply to authentication. The Principles address the intersection of privacy-respecting and security-enhancing practices. The importance of this issue to Canadians requires those who design and implement electronic authentication measures to consider how their systems can best respect privacy at every stage of the process.

The Principles have been developed so as to ensure compatibility with international developments in authentication.

Canada is committed to continued involvement in various international fora addressing the need for global frameworks for authentication. This participation ensures that Canada's approach is in step with other jurisdictions enabling Canadian industry to be competitive in the international marketplace.

Part B: Principles

Principle 1: Responsibilities of Participants

Participants in an authentication process should be aware of the functions they are performing and of the responsibilities associated with those functions. Participants' responsibilities are proportionate to the degree of knowledge and control they can reasonably be expected to have and to exercise.

All participants should act prudently and take reasonable steps to inform themselves of the nature of the authentication process, including its requirements and its limitations, to protect information associated with the process, and to manage the risks to which they are exposed (see Principle 2).

In addition, participants accept the specific responsibilities in connection with the one or more functions they perform:

Authentication Administration

The administrator is responsible for following appropriate and trusted measures so that other participants may have confidence in the credibility of claimed attributes. If any part of the administration function has been delegated to a third party, the administrator is responsible for ensuring that the third party also follows appropriate and trusted processes.

Specification

The specifying participant is responsible for choosing a system such as an authentication infrastructure or process that meets the privacy, security, and other policy and legal requirements associated with an electronic communication. This may include the mechanism by which a participant's authority to enter into the electronic communication, and the integrity of the communication itself, can be ascertained.

End use

The responsibility of end users to inform themselves about the authentication process is limited by the extent of clear and conspicuous information disclosed to them (see Principle 5). The responsibility of end users to protect information relating to the authentication process may be limited by legal or contractual obligations that require disclosure of information concerning the mechanisms they use to determine the reliability of electronic communications.

Standards Development

Standards developers are responsible for ensuring that standards are robust, scalable and adaptive to encourage uniformity in authentication implementations. This responsibility extends to incorporating a wide range of views and best practices into the proposed standards to ensure they are relevant, up-to-date, and continuously applicable. Responsible standards development takes into account both existing and emerging technologies and international practices.

Compliance Assessment

Those who assess compliance are responsible for maintaining and applying a professional and up-to-date level of knowledge and practice so as to be able to provide a reasoned and informed evaluation of authentication processes.

Infrastructure Provision

Infrastructure providers are responsible for following best practices and standards to implement and support the infrastructure that enables authentication.

Principle 2: Risk Management

The risks associated with electronic authentication processes should be identified, assessed and managed in a reasonable, fair and efficient manner.

The responsibilities of participants concerning risk management are proportionate to the degree of knowledge and control that each participant can reasonably be expected to have and to exercise. It is recognized that the ability of participants to identify, assess, and manage risk varies substantially, and that some types of participants (e.g. consumers and small enterprises) cannot reasonably be expected to identify, assess and manage risk to the same extent as participants with access to more significant resources or who define the working relationships. In keeping with the foregoing considerations:

- Risks should be identified to the extent possible. Risks may be material (such as tangible or financial risk including immediate, direct and consequential damages arising from faulty execution or delay in execution) or moral (such as loss of confidentiality or privacy, damages to reputation, theft of identity, etc.).

- Risk should be assessed as to seriousness and potential impact. In assessing risk, special attention should be paid to where and when reliance is placed on the authentication process. In evaluating and assessing risk, it can be helpful to take into account the responsibilities associated with each of the six functions (see Principle 1).

- Risks should be managed to the point of greatest economic efficiency by being assumed, avoided, re-allocated or mitigated. Risk is economically efficient if the residual risk that a participant bears after prudent risk management principles have been applied does not outweigh the benefits gained from participating.

- Contracts may be used to provide a framework for each participant's involvement. Contracts should be clear as to the risks that each party is assuming and should allocate risk in a reasonable, fair and efficient manner. For contracts that are not freely negotiated among equal parties,[1] efforts may be needed to protect the interests of weaker parties.[2]

- Regardless of the means used to allocate risk, the resulting allocation should be reasonable and fair and take into account the ability of participants to manage risk or absorb losses. It should also create incentives for those developing and implementing authentication processes to ensure that their products and services are secure and reliable.

[1] For example, contracts that impose terms of service on users.

[2] Such efforts can be at the industry sector level through the inclusion of provisions in codes or at the government level through policy or legislation.

Principle 3: Security

All participants in an authentication process should be responsible and accountable for security, in proportion to their roles in that process. All participants have a responsibility to contribute to the mitigation of risk through sound security practices. However, infrastructure providers and those involved in authentication administration bear much of the burden to design and maintain systems based on policies and procedures that take into consideration relevant legislation, regulation, policy, industry standards and the socio-cultural environment.[1]

The purpose of information security is to mitigate the risks inherent in the sharing of information electronically. Infrastructure providers and those involved in the specification and administration of authentication processes often take the initiative in designing and implementing security mechanisms, and therefore have an interest in raising awareness by informing other participants about these mechanisms and the participants' role in their maintenance (for example, selecting and safeguarding user passwords). Security mechanisms should conform to applicable, generally accepted standards.

As appropriate, all participants should be made aware and remain conscious, of security risks, known threats and vulnerabilities, and available safeguards. In an authentication process, a security incident that affects a single participant may have implications for all participants. All participants should therefore act at all times to prevent such incidents, and should be ready and able to respond appropriately. Information about known threats, vulnerabilities and risks should be shared amongst participants as appropriate, as an effective preventive measure, to enhance vigilance in detection, and to ensure timely response. Effective information security measures should be proportional to the information risk and respect the rights of participants in keeping with the democratic principles of an open society.

Information technology evolves very rapidly. It is therefore a sound security management practice to ensure that all participants are reliably informed of new and existing threats, and of the role they are expected to play in the prevention, detection and response to security incidents.

The continual review and assessment of security programs is essential to ensure the ongoing efficacy of a security program. Those who establish authentication processes and infrastructure providers in particular, in concert with the other participants in the authentication process, should verify and demonstrate their adherence to sound security management practices, each in proportion to the role they play. A person independent from the authentication process should conduct a periodic review of the security practices associated with the process, and such a review should be integral to any process of accreditation and certification against generally accepted standards.

[1] This security principle accepts and adopts the Organization for Economic Co-operation and Development (OECD) Guidelines for the Security of Information Systems and Networks. The nine principles of the OECD Guidelines are summarized in Part C of this document. The complete text of the OECD Security Guidelines is available online at http://www.oecd.org/pdf/M00034000/M00034292.pdf, as are references to pertinent international standards on IT security, authentication audit, accreditation and certification guidelines, and other material of interest with respect to the security of authentication processes.

Principle 4: Privacy

All organizations engaged in the design or operation of authentication processes should, at a minimum, comply with the data protection standards set out in applicable legislation, jurisprudence, and codes of practice ("privacy laws and codes").[1] In particular, the collection, use and disclosure of personal information[2] in the authentication context should be minimized.

Identity-based authentication can conflict with privacy considerations. Stronger authentication, for example, may require the collection and comparison of more personal information. However, minimization of the collection, use and disclosure of personal information in the authentication context is fundamental for security as well as privacy reasons. Privacy safeguards can actually contribute to the security of authentication processes.

Authentication Administration

Authentication administration should involve the collection of personal information only where necessary. Any personal information collected should be used for no purpose other than authentication. Authentication of a business should focus on business attributes rather than personal attributes of individual employees.

If collection of personal information is required, such collection should be minimized. Any retention, use or disclosure of personal information should also be minimized.

Personal information should be collected, retained, used or disclosed only with the informed consent of the individual.

Specification and Infrastructure Provision

Authentication processes should be designed to require that the least possible personal information be collected, used and disclosed. Process design should take into account the access rights of participants and the obligation of organizations to make information available about their privacy policies. Organizations using authentication processes designed by others have a responsibility to ensure that those processes respect privacy.

End Use

End users of authentication processes and services should take reasonable measures to ensure that personal information within their control is protected from unauthorized collection, use or disclosure.

Standards Development

Authentication standards should be developed in full accordance with the privacy principles set out in privacy laws and codes. Privacy protection should explicitly be built in to authentication standards. Standards developers should consider the coincidence of measures that contribute to protection of data privacy with those designed to ensure security of authentication processes.

Compliance Assessment

Compliance assessment should include assessment of whether and how the entity in question is complying with the privacy principles set out in laws and codes. Compliance assessors should protect the confidentiality of personal information they deal with in the context of their assessments, in accordance with privacy laws and codes.

[1] General private sector data protection legislation currently in force includes the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), and the Quebec *Act respecting the protection of personal information in the private sector* (Bill 68). Provinces other than Quebec may also enact general data protection legislation. Federal/provincial public sector privacy legislation and sector-specific legislation protecting personal information may also apply.

The CSA Model Code for the Protection of Personal Information, CAN/CSA-Q830-96 has been incorporated in the federal *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 ("PIPEDA"), as Schedule 1 to that Act. This Code was developed by a multi-stakeholder working group and adopted by the Standards Council of Canada as a national standard in 1996. Many industry Codes of Practice also address data protection.

[2] as defined in the PIPEDA: "any information about an identifiable individual".

Principle 5: Disclosure Requirements

Participants that offer authentication services should disclose information to the other participants to ensure that all participants are aware of the risks and the responsibilities associated with participation.

The information disclosed should include policies, practices and procedures and include information about whether services are periodically reviewed or audited.

Appropriate disclosure requires information to be provided in sufficient detail for the purpose, be in plain language and be conspicuous. All three factors will have a bearing on the knowledge of the disclosed information that other participants can reasonably be expected to have.

Disclosure should *not* include security-related information that, if disclosed, would introduce vulnerabilities and increase risk. However, the amount and nature of information disclosed should be sufficient for participants to understand their responsibilities and to make informed risk management decisions concerning reliance on the authentication. The extent and nature of the information may vary depending on whether the end user is an individual or an organization.

Participants should be notified of the availability of information and of any changes to the information. Evidence of receipt of notification may be required depending on the nature of the authentication process and associated applications.

Participants that offer authentication services should disclose their policy and practices concerning the collection of personal information. The Privacy Principle more fully addresses personal information and its disclosure (see Principle 4).

Disclosure requirements should be considered in conjunction with Principle 1 (Responsibilities) and Principle 2 (Risk Management).

Principle 6: Complaints Handling

Whenever authentication processes or services are implemented, a complaints-handling process should be available that enables participants to resolve complaints efficiently and effectively and to respond appropriately to non-compliance issues.

Complaints-handling processes should incorporate the following principles:

Visibility
Information about how and where to direct complaints should be well publicized to all participants and their personnel and to other interested parties, and should include full information about the complaints-handling process.

Accessibility
A complaints-handling process should be easily accessible to all participants, and should ensure that information is readily available on the details of resolving disputes. For individuals with complaints, the process and supporting information should be easy to understand and use, be in plain language and be available in the languages in which the products and services were originally offered.

Responsiveness
Complaints should be dealt with promptly and thoroughly. Complaints should be assessed from a security perspective and resolved in priority according to their potential negative impact on the participants involved or on the authentication implementation as a whole.

Fairness and Objectivity
Each complaint should be addressed in a balanced manner through the complaints handling process and should be fair to the complainant and the participant against whom the complaint is made.

Charges
Access to the complaints-handling process should be free of charge to the complainant unless charges have been identified and agreed to in advance by the complainant.

Confidentiality and Privacy
Personal information concerning complainants should be available only where needed within the organization and must be actively protected from disclosure unless the complainant expressly consents to its disclosure.

Accountability
Organizations offering authentication services should ensure that there is an identified individual or identifiable unit within the organization responsible for the systematic recording of complaints and outcomes and reporting on the actions and decisions of the organization with respect to complaints handling.

Continual Improvement
Continual improvement of the quality of authentication products and services is facilitated through the complaints-handling process based on customer and other feedback. The complaints handling process itself should be monitored on an ongoing basis and reviewed and assessed in light of feedback.

Unresolved Complaints
Where complaints cannot be resolved internally, organizations should be willing to use appropriate third-party dispute resolution processes upon request by the complainant, including those administered by private third parties. However, complainants should continue to have access to the justice system.

Part C: Additional Information/References

1. Additional Information

OECD Guidelines for the Security of Information Systems and Networks

i. ***Awareness***
Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

ii. ***Responsibility***
All participants are responsible for the security of information systems and networks.

iii. ***Response***
Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents.

iv. ***Ethics***
Participants should respect the legitimate interests of others.

v. ***Democracy***
The security of information systems and networks should be compatible with essential values of a democratic society.

vi. ***Risk assessment***
Participants should conduct risk assessments.

vii. ***Security design and implementation***
Participants should incorporate security as an essential element of information systems and networks

viii. ***Security management***
Participants should adopt a comprehensive approach to security management.

ix. ***Reassessment***
Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

2. References

GENERAL

Domestic - Background:

Industry Canada Electronic Commerce Policy - Authentication
http://e-com.ic.gc.ca/english/authen/index.html

Canada's Cryptography Policy
Government of Canada, 1998
http://e-com.ic.gc.ca/english/crypto/631d11.html

Domestic - Related Initiatives and Reference Documents

a) General

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, Part 2
http://laws.justice.gc.ca/en/2000/5/index.html

Uniform Electronic Commerce Act
Uniform Law Conference of Canada
http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1

*Act to establish a legal framework for information technology (*2001)
Province of Quebec
http://www.autoroute.gouv.qc.ca/loi_en_ligne/loi/texteloi.html

Current Statutory Initiatives in Canada: Electronic Commerce (Department of Justice Canada)
http://canada.justice.gc.ca/en/ps/ec/sriec.html

Government of Canada Treasury Board, Policy on Electronic Authorization and Authentication
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/tbm_142/2-2_e.asp

Government of Canada Treasury Board, PKI Management Policy
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki_e.asp

Government of Canada Digital Signature Certificate Policies
http://www.cio-dpi.gc.ca/pki-icp/guidedocs/ds-cert-policy/introduction_e.asp

*Voluntary Codes: A Guide for their Development and Use (*1998)
Government of Canada (Industry Canada and Treasury Board)
http://strategis.ic.gc.ca/SSG/ca00863e.html

b) Consumer Protection

Principles of Consumer Protection for Electronic Commerce (1999)
Industry Canada
http://strategis.ic.gc.ca/SSG/ca01185e.html

Canadian Code of Practice for Consumer Protection in Electronic Commerce (2003)
Industry Canada
http://strategis.ic.gc.ca/pics/ca/eng_consumerprotection03.txt

Canadian Code of Practice for Consumer Debit Card Services (1996, rev. 2002*)*
Industry Canada
http://strategis.ic.gc.ca/SSG/ca01581e.html

International - Related Initiatives and Reference Documents

Directive 1999/93/EC on a Community framework for electronic signatures (1999)
The European Parliament and the Council of the European Union
http://europa.eu.int/ISPO/docs/policy/docs/399L0093/en.pdf

OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (2000)
http://www.oecd.org/EN/document/0,,EN-document-44-1-no-20-320-0,00.html
http://www.olis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-cp(2002)4-final

International Consensus Principles for Electronic Authentication (1999)
Internet Law and Policy Forum
http://www.ilpf.org/events/intlprin.htm

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (1999)
The Internet Engineering Task Force
ftp://ftp.isi.edu/in-notes/rfc2527.txt

Electronic Authentication: Issues Relating to its Selection and Use (2002)
Asia-Pacific Economic Co-operation
http://www.apectelwg.org/apecdata/telwg/eaTG/EA_text.pdf

UNCITRAL Model Law on Electronic Signatures (2001)
http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf

Global Business Dialogue
http://www.gbde.org/authentication.html

Digital Signature Guidelines (1996)
American Bar Association
http://www.abanet.org/scitech/ec/isc/dsgfree.html

PRINCIPLES

Principle 1: Responsibilities of Parties

Standards for a Global Digital Marketplace: A Canadian Standards Framework for Electronic Commerce (1998)
http://e-com.ic.gc.ca/english/strat/doc/standards.pdf

Principle 2: Risk Management

BITS Framework for Managing Technology Risk for Information Technology (IT) Service Provider Relationships (2001)
BITS Financial Services Roundtable
http://www.bitsinfo.org/FrameworkVer32.doc

Electronic Commerce: Who Carries the Risk of Fraud (2000)
Foundation for Information Policy Research, U.K.
http://elj.warwick.ac.uk/jilt/oo-3/bohm.html

Principle 3: Security

OECD Guidelines for the Security of Information Systems and Networks (2002)
Organization for Economic Co-operation and Development
http://www.oecd.org/pdf/M00034000/M00034292.pdf

GOC Information Technology Security Standard
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON-1_e.asp

GOC PKI policies and methodologies
http://www.cio-dpi.gc.ca/pki-icp/index_e.asp
http://www.cio-dpi.gc.ca/its-sti/index_e.asp

AIPCA/CICA Trust Services
www.aicpa.org/assurance/webtrust/princip.htm

PKI Assessment Guidelines (2001)
American Bar Association
http://www.abanet.org/scitech/ec/isc/pagv30.pdf

ISO 17799 Code of practice for information security management (2000)
http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=

ISO TR 13335 Guidelines for the management of IT security
http://www.iso.org/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=13335

EESSI European Electronic Signatures Standards Initiative
http://www.ictsb.org/eessi/EESSI-homepage.htm

Principle 4: Privacy

Personal Information Protection and Electronic Documents Act, *S.C. 2000, c. 5, Part 1*(2000)
Government of Canada
http://laws.justice.gc.ca/en/2000/5/index.html

*Authentication Through the Lens of Privacy (*2003)
National Academies - U.S., Computer Science and Telecommunications Board
http://www.nap.edu/books/0309088968/html/

Webtrust Program for Online Privacy (2000)
American Institute of Certified Public Accountants (AICPA)/Canadian Institute of Chartered Accountants (CICA)
http://www.aicpa.org/webtrust/execsumm3.htm

Privacy and Public Key Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals (2001)
Office of the Federal Privacy Commissioner, Australia
http://www.privacy.gov.au/publications/pki.pdf.

Principle 5: Disclosure Requirements

Principles of Consumer Protection for Electronic Commerce (1999)
Industry Canada
http://strategis.ic.gc.ca/SSG/ca01185e.html

Principle 6: Complaints Handling

ISO Committee Draft, ISO/CD 10018: Complaints Handling
International Organization for Standardization
http://www.iso.org/iso/en/commcentre/news/2002/iso10018.html

AS/NZS 4269 *Complaints Handling*
http://www.standards.com.au/catalogue/script/Details.asp?DocN=stds000012657