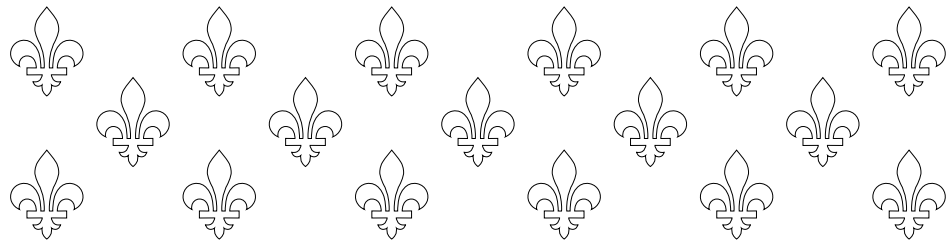

NATIONAL ASSEMBLY

FIRST SESSION THIRTY-SIXTH LEGISLATURE

Draft Bill

An Act respecting the legal normalization of new information technologies

Tabled by
Mr David Cliche
Minister for the Information Highway and Government Services

Québec Official Publisher
2000

EXPLANATORY NOTES

The object of this draft bill is, principally, to provide for the legal security of documentary communications, the functional equivalence of documents and recognition of their legal value regardless of the medium used, and the interchangeability of media. The draft bill also promotes concerted action to harmonize the technical systems and standards used in communications involving technological documents.

The draft bill first states that, except where otherwise required by law, a document may be in any medium. The reliability of a document is based on its integrity, which must be maintained throughout its life cycle if the document is to retain its legal value. The draft bill recognizes that a reliable document has full legal value, regardless of the medium used, and sets out the rules of proof that apply, according to the reliability of the document, the rules governing information transfers, the rules concerning the retention, consultation and transmission of documents, and the responsibilities of the various intermediaries offering communication network services.

The draft bill provides for various ways of authenticating the identity of a person communicating by means of a technological document, and related measures to ensure confidentiality. It also states the necessity of linking a person to a document expressing the will of that person, and provides for measures to establish such links, including provisions to regulate the offer of certification and directory services. Every provider of certification services in Québec or elsewhere will be able to receive accreditation from a person or body determined by the Government.

To promote the harmonization of systems, norms and technical standards, the draft bill requires the Government to set up a multidisciplinary committee to examine the compatibility and interoperability of media and information technologies.

Last, the draft bill contains interpretative, amending and final provisions for the purpose of its application.

LEGISLATION AMENDED BY THIS DRAFT BILL :

– Civil Code of Québec ;

– Act respecting Access to documents held by public bodies and the Protection of personal information (R.S.Q., chapter A-2.1) ;

– Archives Act (R.S.Q., chapter A-21.1) ;

– Code of Penal Procedure (R.S.Q., chapter C-25.1) ;

– Real Estate Brokerage Act (R.S.Q., chapter C-73.1) ;

– Interpretation Act (R.S.Q., chapter I-16) ;

– Consumer Protection Act (R.S.Q., chapter P-40.1).

Draft Bill

AN ACT RESPECTING THE LEGAL NORMALIZATION OF NEW INFORMATION TECHNOLOGIES

THE PARLIAMENT OF QUÉBEC ENACTS AS FOLLOWS:

CHAPTER I

GENERAL PROVISIONS

1. The object of this Act is to ensure

(1) the legal security of documentary communications between persons, associations, partnerships and the State, regardless of the medium used;

(2) the coherence of legal rules and their application to documentary communications using information technology media, whether electronic, magnetic, optical, wireless or other, including microform and combined technologies, the documents involved being referred to as technological documents in this Act;

(3) the functional equivalence of documents and the recognition of their legal value, regardless of the medium used, and the interchangeability of media and technologies;

(4) the link between a person and a technological document, as indicated by any means allowing them to be associated, such as a signature, or any means allowing them to be identified and, if need be, located, such as certification;

(5) concerted action for the harmonization of the technical systems and standards involved in the communication of technological documents and the interoperability of media and technologies.

2. Except where a document is required by law to be in a specific medium, a document may be in any medium. A requirement that a document be in writing does not entail the use of a specific medium.

Any medium and any technology may be used, provided the choice of medium and technology complies with the rule of law.

CHAPTER II

DOCUMENT

DIVISION I

CONCEPT OF DOCUMENT

3. Information delimited or structured, according to the medium used, by tangible or logical features that is intelligible in the form of writing, images or sound, constitutes a document. A document may be drafted using any type of writing, including a system of symbols that may be transcribed into writing, images or sounds or another system of symbols.

A database whose structural features allow the information contained in the database to be delimited and structured is also considered to be a document.

4. A document must, even if it is fragmented and dispersed in one or more media at one or more locations, be considered to form a whole where its tangible or logical structural features allow the fragments to be connected, directly or by reference, and where the elements ensure both the integrity of each fragment and the integrity of the reconstituted document as it existed prior to its fragmentation and dispersal.

Conversely, separate documents, even when combined into a single document for transmission or retention purposes, do not lose their distinct nature, where their tangible or logical structural features ensure both the integrity of the combined document and the integrity of each reconstituted document making up the whole.

DIVISION II

RELIABILITY

5. A document is reliable where its components are delimited and structured in such a way as to ensure the integrity of the document over its entire life cycle, from its creation, in the course of transfer, consultation or transmission, and until its retention, including its storage, or its destruction.

The integrity of a document is assured where it is possible to verify that the information it contains has not been altered and has been maintained in its entirety, and where the medium in which the information is contained provides stability and the required perennity.

In assessing the integrity of a document, the security measures taken to protect the document during its life cycle shall be taken into account.

6. The Government may, by regulation, prescribe security measures to assure document integrity and, for that purpose, the cases and conditions in which specific media or technologies may or must be used.

7. The fact that documents containing the same information in different media show differences in the way in which the information is stored or presented, or include information that is clearly or implicitly different in relation to the medium or the security of the documents, does not affect the integrity of the documents.

Similarly, differences relating to page numbering, the tangible or intangible nature of pages, format, recto or verso presentation, total or partial accessibility, and sequential or thematic information retrieval possibilities, do not affect the integrity of the documents.

DIVISION III

DETERMINATION OF LEGAL VALUE OF DOCUMENT

8. A reliable document, regardless of its medium, has full legal value.

The document may constitute a means of proof and be admitted as documentary evidence or, if the document contains intelligible information in the form of sounds or images, as real evidence.

A document whose reliability may be neither confirmed nor denied may, depending on the circumstances, be admissible as testimonial evidence or real evidence and serve as commencement of proof.

9. Two or more documents in different media may have the same legal value if each is reliable and contains the same information. One document may be substituted for another and they may be used simultaneously or in alternation. In addition, each such document may be used for the same purposes, in particular, as an original or as a copy standing in lieu of an original.

If one document is lost, it may be reconstituted using another document.

10. In the event of a divergence between the information contained in a document transferred from paper to another medium and the information contained in the resulting document, the paper document shall prevail.

In the event of a divergence between two documents in different media or using different technologies that purport to contain the same information, the document containing information that is verifiably unaltered and maintained in its entirety shall prevail.

If the above rules do not allow the document that prevails to be determined, and in the absence of an agreement or understanding, the document that appears in the circumstances to be the most reliable shall prevail.

11. Where a technological document must have the value of an original to assure that the document is the first form from which copies are made, that the

document is unique or that it is the first form of a document associated with a person, the document meets the requirement if the integrity of the document is assured and if

(1) in the first case, the components of the source technological document were identified upon reproduction and have been retained intact;

(2) in the second case, the components of the document or its medium are structured using a process that makes it possible to assure that the document is unique, in particular through the inclusion of an exclusive or distinctive component or the exclusion of any form of reproduction;

(3) in the third case, the components of the document or its medium are structured using a process that makes it possible to assure that the document is unique, to identify the person with which the document is associated and to maintain the association during the entire life cycle of the document.

The processes referred to in subparagraphs 2 and 3 of the first paragraph must be recognized by a national or international standards agency referred to in section 69.

12. Where a document must be sealed using a seal, signet, press, stamp or other instrument to authenticate the document as an original, the requirement may be satisfied in the case of a technological document if a process allows the integrity of the document to be assured.

However, where a document must be authenticated as an original, the form of the document must have the characteristic features of the medium containing the information, such as the use of specially grained paper, the affixing of a distinctive mark or mention or the use of a process that allows such affixing.

13. Where the production of a copy of a technological document is permitted, the process used to make the copy must offer a sufficient guarantee to assure the integrity of the copy and that it contains the same information as the source document.

In assessing the integrity of a copy, the circumstances in which it was made shall be taken into account, and the fact that it was made systematically and without interruption or by means of a process based on technical norms or standards recognized by a national or international standards agency referred to in section 69.

However, as regards its form, a copy must include characteristic features to show that it is a copy, such as an indication of the place and date on which the copy was generated, a statement that it is a copy, or any other feature.

A copy shall be presumed reliable as regards third parties by the sole fact that it was generated by an enterprise within the meaning of the Civil Code or by the State.

14. Where a copy of a document must be certified or authenticated, the requirement may be satisfied in the case of a technological document, not only by visual or manual comparison, but also by means of a comparison process that recognizes whether the information in the copy is identical to the information in the source document, or that their respective imprints are identical.

15. It is not necessary to prove the reliability of a document unless the person contesting its reliability establishes, upon a preponderance of evidence, that the integrity of the document has been affected.

16. The processes, systems or technologies used to communicate by means of technological documents need not be proved, even where the reliability of a document is contested, provided they are described in an order of the Government made after consulting the committee referred to in section 67, with an indication of their application, the duration of their use and the norm or standard concerned.

However, the exemption does not prevent a person contesting the reliability of a document from establishing, upon a preponderance of evidence, an error in the use or dysfunction in the application of such processes, systems or technologies.

DIVISION IV

RELIABILITY AND LIFE CYCLE OF DOCUMENTS

§1. — *Transfer of information*

17. Except in the case provided for in section 19, before a document, whether an original or a copy, containing information that has been transferred to another medium using a different technology can be destroyed, or replaced by a document resulting from the transfer containing the same information, the transfer must

(1) in the case of a legal person, partnership or association or of the State, have been authorized by a person in authority or responsible for the retention of the document, and be supported by documentation that can be produced as evidence;

(2) in the case of an individual, be preceded by a verification of the fact that the medium and technology available to the individual for the transfer guarantee the preservation of the information transferred and guarantee the integrity of the document to be transferred, if it is not destroyed, and the document resulting from the transfer; no documentation other than the documentation of the suppliers may be required to be produced as evidence in connection with the medium or technologies available to the individual, subject to a regulation made under section 20.

18. The documentation referred to in paragraph 1 of section 17 must, at least,

(1) allow the identification of the document to be transferred;

(2) state the process used in the transfer, which must be based on technical norms or standards recognized by a national or international standards agency referred to in section 69;

(3) include a register of dysfunctions that occurred during the transfer and the corrective measures taken;

(4) be updated, in particular, to reflect the changes that may be made to the transfer process, and the inspections and security checks made during the time when the document was in the receiving medium;

(5) be supported by a statement of transfer made by the person who supervised the transfer, attesting that authorization was given for the transfer, that the transfer process used complied with the standards and was correctly applied, that the transferred document was not altered during the transfer and that both documents contain the same information.

The documentation and statement shall be joined, directly or by reference, to the document resulting from the transfer, to its structural features or to the medium. They shall be retained during the life cycle of the document.

19. Where the information is transferred to paper, the two documents must be compared in order to affirm that the paper document contains the same information as the technological document before the latter is destroyed. The comparison may take place on-site or by remote access, using a process appropriate to the medium of the transferred document or a visual or manual comparison of the paper document and technological document.

In addition, the person who effects the transfer must indicate on the resulting document that a transfer has taken place and affix, directly or by reference, a transfer statement stating that the document resulting from the transfer contains the same information as the transferred document.

20. All additional documentation that may be required because of the use of a specific medium or technology, able to establish that the document resulting from the transfer contains the same information in the receiving medium, shall be determined by government regulation.

21. A document resulting from a transfer and that is reliable is admissible as evidence and has the same evidentiary weight as the transferred document, whether or not the latter document has been destroyed.

§2. — *Retention of document*

22. Every person must, while required to retain a document, ensure that its integrity is maintained and see to it that equipment is available to make it accessible and intelligible and usable for the purposes for which it is intended.

23. Documents that are required by law to be retained may be destroyed once they have been transferred. However, before destroying such a document, the person responsible for it shall

(1) ensure that the transfer statement has been made, where applicable;

(2) keep and maintain a destruction schedule for transferred documents, except if the person is an individual;

(3) ensure the protection of any confidential and personal information contained in the documents to be destroyed;

(4) complies with the additional requirements prescribed by government regulations;

(5) ensure that the documents, if they are in the possession of the State or of a legal person established in the public interest, are destroyed in accordance with the retention schedule established under the Archives Act (R.S.Q., chapter A-21.1).

However, a document that, in its original medium, has archival, historical or heritage value that meets the criteria for recognition determined by government regulation must be retained even if it has been transferred.

24. A person responsible for retaining a technological document must, in order to preserve its integrity when the information it contains is modified, record the details determining who made the request for modification, and when, by whom and why the modification was made. The detail forms an integral part of the document even if they are recorded in a separate document.

25. An intermediary who offers document retention services on a communication network is not responsible for the activities engaged in by a service user using the documents retained by the service user or at the service user's request.

However, the service provider may become responsible for such activities if, upon becoming aware that the documents are being used for an illicit activity, or of circumstances that make such a use apparent, the service provider does not act promptly to block access to the documents or otherwise prevent the pursuit of the activity.

Similarly, an intermediary who offers documentary referral services, such as an index, hyperlinks, lists or research tools, is not responsible for the

activities engaged in using those services. However, the service provider may become responsible if, upon becoming aware that the services are being used for an illicit activity, the service provider does not act promptly to cease providing services to persons known by the service provider to be engaging in such an activity.

§3. — *Consultation of document*

26. Every document to which a person has a right of access must be intelligible, either directly or with the assistance of a device or using structural features that give access to the document.

A right of access may be satisfied by access to a copy of the document or to a document resulting from a transfer.

The medium of access must take into account the wishes of the person having a right of access to the document, unless the medium chosen would involve substantial practical difficulties such as cost and the need to transfer information.

27. To ensure that the purpose for which a technological document containing personal information is made public is respected, the use of extended search functions must be authorized by the person responsible for access to the document; the person may set conditions for the use of such functions.

However, the criteria on which the use of extended search functions for such technological documents may be authorized shall be determined by government regulation.

28. The person responsible for access to a technological document containing confidential information must take appropriate security measures to ensure its confidentiality, either by providing controlled access by means of a reduced visibility method, or a method that prevents an unauthorized person from acquiring knowledge of such information or, as the case may be, from otherwise gaining access to the document or to the components giving access to the document.

The cases in which access to or consultation of a technological document must be detected, and the cases in which a particular means of detection such as a log must be used, shall be determined by government regulation.

29. While a document is in the custody of a service provider, the service provider is required to assure its security, to ensure its integrity and, where applicable, to protect its confidentiality and prevent access by unauthorized persons.

The service provider must, in addition, ensure compliance with any other obligation provided for by law in relation to the retention of the document.

30. An intermediary who provides communication network services or who retains or transmits documents on a communication network is not required to check the information contained in the documents or to identify circumstances indicating that the documents may be used for illicit activities.

However, the intermediary may not take measures to prevent the person responsible for access to documents from exercising his or her functions, in particular as regards confidentiality, or to prevent the competent authorities from exercising their functions as regards public security or the prevention, detection, proof and prosecution of offences.

§4. — *Transmission of document*

31. A document may be transmitted by any means appropriate to its medium, unless the law requires the exclusive use of a specific means of transmission.

Where an Act provides for the transmission, sending or forwarding of a document by mail or courier service, the document may be transmitted, sent or forwarded by means of the technology appropriate to the medium of the document to be transmitted.

32. The selected means of transmission must allow the integrity of the transmitted document to be preserved to ensure that the technological document received has the same value as the transmitted document. The documentation establishing the ability of a means of transmission to preserve the integrity of both the transmitted and the received document must be available for production as evidence, where applicable.

The sole fact that a document is fragmented, compressed or stored during its transmission for a limited time to improve the efficiency of the transmission does not entail the conclusion that the document's integrity has been affected.

33. A technological document is presumed transmitted, sent or forwarded when the action required to send it to the receiver is accomplished by or on the instructions of the sender, and the transmission cannot be stopped or, if it can still be stopped, is not stopped by or on the instructions of the sender.

The document is presumed received or delivered when it becomes accessible in intelligible form at the address indicated by the receiver as the address where the receiver accepts the receipt of documents from the sender, or at the address that the receiver publicly represents as the address where the receiver accepts the receipt of documents.

The time of sending or of receipt may be established by a transmission slip or acknowledgement of receipt or by the supplying of information kept with the document and capable of indicating the source, path and destination of the document or the date, hour, minute and second of sending and receipt, or by any other agreed method.

34. In no case may the acquisition of a specific medium or technology to transmit or receive a document be required, unless expressly provided by law or by an agreement.

Similarly, in no case may the reception of a document in a medium other than paper, or by means of a technology that is not at the receiver's disposal, be required.

A product or service, or information on a product or service, that is available in more than one medium, may be obtained in any such medium.

35. Where a document is a technological document, a requirement under an Act for several copies of the document to be transmitted, sent, forwarded or remitted to a single receiver is satisfied by the submission of a single copy.

However, a sender who sends more than one copy must be in a position to verify the integrity of the other copies generated by the sender's or the user's system or from a document, including software, placed at the sender's disposal by the receiver.

In addition, a receiver who generates a copy must be in a position to guarantee its integrity.

36. A presumption of reliability exists in favour of an individual where a copy of a document of an enterprise, within the meaning of the Civil Code, or a document in the State's possession is generated by a system or from a document, including a program, placed at the sender's disposal by the enterprise or the State.

37. Where the information contained in a document is declared by law to be confidential information, confidentiality must be protected by a means appropriate to the mode of transmission, including on an open or closed communication network.

The confidentiality of a transmitted document may also be protected by the encryption of the document before it is transmitted, by the use of communications channels equipped with encryption functions, by the use of communications channels under the responsibility of a person that are dedicated to the transmission of the person's documents or documents from persons to whom the person has given access to the channel, or by any other means agreed between the sender and the receiver.

The documentation explaining the agreed mode of transmission must be available for production as evidence.

38. A party that communicates by means of a pre-programmed document that interacts without the assistance of a natural person must, on pain of non-enforceability, ensure that the document provides the necessary instructions to allow the other party to advise the sending party of an error as soon as

possible or prevent or correct an error, to avoid receiving an unwanted product or service, or avoid receiving an unwanted product or service because of the error, or to return or, where applicable, destroy the product received.

39. An intermediary who provides communication network services exclusively for the transmission of documents is not responsible for the acts performed by others by means of the documents transmitted or retained during the normal course of the transmission and during the time required to ensure the effectiveness of the transmission.

The intermediary may become responsible if the intermediary is the sender of a document, selects or alters the information in the document, selects the person who transmits, receives or has access to documents, retains the document longer than is necessary for its transmission, or otherwise participates in the acts performed by others.

40. An intermediary who, as part of the transmission services provided by the intermediary via a communication network, maintains documents provided by a client on the network for the sole purpose of ensuring the effectiveness of their subsequent transmission to the persons entitled to access to the information, is not responsible for the acts performed by others by means of those documents.

The intermediary may become responsible for such acts, in the cases referred to in the second paragraph of section 39, or if the intermediary does not comply with the conditions of access to the document, takes steps to prevent the verification of who has had access to the document, does not withdraw a document from the network or block access to the document after becoming aware that the document has been withdrawn from its initial position on the network because the persons entitled to access the document are unable to gain access or because a competent authority has ordered that the document be withdrawn from the network or that access to the document be blocked.

CHAPTER III

LINKS BETWEEN PERSONS AND TECHNOLOGICAL DOCUMENTS

DIVISION I

MEANS OF LINKING PERSONS AND TECHNOLOGICAL DOCUMENTS

41. The link between a person and a technological document may be established by any process or combination of processes, to the extent that they allow

(1) confirmation of the identity of the person, of the person's association with the document and, if need be, of the person's location;

(2) identification of the document and, if need be, of its origin, path and destination at a given time.

42. The link between a person and a document may be established by means of a signature.

Whatever the medium, a signature is valid if the signing process satisfies the requirements of article 2827 of the Civil Code.

43. The signature of a person affixed to a technological document may be set up against that person where the document is a reliable document and the link between the signature and the document, at and from the time of signing, is ensured.

44. An asymmetric encryption system may be used to affix a signature or otherwise establish a link between a person and a document.

Within the asymmetric encryption system, a person holding a key pair who uses a private key to sign or decrypt a document is presumed to be the person corresponding to the public key connected to the private key, whose identity is indicated in the certificate or, as the case may be, the directory referred to in Division III, unless the party contesting that fact establishes, upon a preponderance of evidence, that at the time of signing or decryption, another person used the person's private key without entitlement, that the signature of the holder of the public key has been usurped, or that the confidentiality of the private key has been affected in some way.

The person identified in a certificate as the holder of a key pair is presumed to have a link with any document signed or decrypted by means of the private key indissociably linked to the public key.

A person providing certification services using such a system must be able to confirm the link between the person or object and the public key assigned to that person or object.

DIVISION II

IDENTIFICATION AND LOCATION OF PERSONS, DOCUMENTS AND OTHER OBJECTS USED FOR COMMUNICATION

§1. — *Persons*

45. A person who, following verification, is able to confirm the identity of a person may do so by means of a document, such as a certificate, that must be reliable and must protect the confidential information it may contain. The document may be transmitted in any medium.

A person's identity may be verified by reference to the registers provided for in the Civil Code or the Act respecting the legal publicity of sole proprietorships, partnerships and legal persons (R.S.Q., chapter P-45), which establish a person's identity regardless of the medium used to communicate. The person's identity may also be verified on the basis of the person's characteristics or knowledge or of the objects in the person's possession.

The verification may be carried out by or for a person on the premises or by remote access, by direct observation or by means of such reliable documents as may be available in different media for consultation on the premises or by remote access.

46. The use, as proof of identity, of a technological document containing a personal characteristic or particular information or that indicates that the person to be identified possesses a particular object requires that the integrity of the document presented be preserved.

Such a document must, in addition, be protected from interception where its retention or transmission via a communication network makes it possible to usurp the identity of the person referred to in the document. Its confidentiality must be protected, where applicable, and its consultation must be logged.

47. Where an attestation, card, certificate, identity document or other document is required by law to establish the identity of a person, the requirement must be interpreted as allowing the document to be provided by means of the technology appropriate to the medium concerned.

48. Where the consent of a person is required by law for the performance of an act by means of a technological document, the identity of the person must be established before the act is performed and the process used to express consent must not allow repudiation on grounds of mistaken identity.

49. Unless otherwise expressly provided by law, no person may require a person's identity to be established by means of a process or device that allows the person to be located at any time and in any place, or that affects the person's physical integrity.

50. No person may require a person's identity to be verified or confirmed by means of a process that allows biometric characteristics or measurements to be recorded.

Where a person expressly consents to having his or her identity established in such a manner, only the minimum number of characteristics or measurements needed to link the person to the act performed, and that are among the characteristics or measurements that may not be recorded without the person's knowledge, may be used.

No other information concerning the person that could be revealed by the characteristics or measurements recorded may be used for any other purpose than the verification or confirmation of the person's identity. Such information may only be disclosed to the person concerned, at the person's request. Similarly, no decision concerning the person that relates to a matter other than the establishment of the person's identity may be made on the basis of such characteristics or measurements.

The characteristics or measurements and any note made concerning them must be destroyed when the object of the verification or confirmation of identity has been met or when the reason for the verification or confirmation no longer exists.

The creation of a database of biometric characteristics and measurements must be disclosed to the Commission d'accès à l'information which may make orders concerning the database to determine how the database is to be set up, used, consulted and retained, and how the measurements or characteristics recorded to establish a person's identity are to be stored and destroyed.

§2. — *Documents and other objects*

51. Where a document used for a network communication is retained for production as evidence, the person responsible for the document must store its identifier with it during its entire life.

The identifier must be accessible through a directory service, one of the functions of which is to associate an identifier with its location. The association between an identifier and an object may be guaranteed by a certificate which is itself accessible through a directory service that may be consulted by the public.

An identifier shall comprise a distinct and unambiguous reference name in the local nominative space where it is registered, along with the necessary extensions to link the name to other designations that allow it to be located within a universal nominative space.

To allow the origin, path or destination of a document at any given time to be established, the other objects used to transmit the document, such as public key certificates, algorithms, servers, and routing and switching devices, must be able to be identified and located, by means of the identifiers assigned to each object.

DIVISION III

CERTIFICATION

§1. — *Certificates and directories*

52. A certificate may be produced as evidence, in any appropriate medium, to establish one or more facts including the confirmation of a person's identity, the accuracy of the identifier of a document or other object, or the link between a person and a document or other object; the certificate may be a public key certificate attesting to the validity of a private key associated with both a person and a document, or a certificate confirming the existence of certain attributes of a person or object.

An attribute certificate may establish, in particular, a person's function, capacity, rights, and powers or privileges within a legal person, association, partnership or the State or within an employment position. The certificate may also confirm the information used to identify and locate an object, associate it with a public key, determine its use or the right of access to the object or any other related right or privilege.

Access to an attribute certificate relating to a person must be authorized by the person or by a person having authority over the person.

53. A certificate may be joined directly to another document used in a communication or be made accessible through a directory that is itself accessible to the public.

A certificate must include at least the following information:

(1) the distinctive name and signature of the service provider issuing the certificate;

(2) a reference to the policy statement of the certification service provider, describing its practices, on which the guarantees offered by the certificate are based;

(3) the version and serial number of the certificate;

(4) the beginning and the end of the valid period of the certificate;

(5) in the case of a certificate confirming the identity of a person or the accuracy of an object identifier, the distinctive name of the person or object identifier;

(6) in the case of an attribute certificate, a description of the attribute whose existence is confirmed by the certificate and the identification of the person or object to which it is linked;

(7) in an asymmetric encryption system, the numerical value of the public key assigned to the person or object and the identifier of the algorithm that allows the key to be used.

54. Where the certificate is issued to a legal person, to a partnership or association or to the State, it must allow the natural person who, where applicable, holds the private key linked to the public key mentioned in the certificate to be identified.

The distinctive name of the natural person may be a pseudonym, but the certificate must indicate if that is the case. Certification services are required to communicate the name of the person corresponding to the pseudonym to any person legally authorized to obtain that information.

55. A directory whose function is to identify or locate a person or object or to establish a link between a person and an object must be constituted in accordance with the norms or standards recognized by a national or international standards agency referred to in section 69.

The directory must be accessible to the public, either directly or by means of a device, or by means of an access procedure to various domains of a network where confirmation of the validity of an identifier, certificate or other information included in the directory may be obtained.

However, the directory may not make public the reasons for which a certificate has been suspended or cancelled.

§2. — *Certification and directory services*

56. Certification and directory services may be offered by a person or by the State.

Certification services involve verifying the identity of persons and issuing certificates to confirm their identity or the accuracy of the identifier of an object. Directory services involve entering certificates and identifiers in a directory that is accessible to the public and confirming the validity of the certificates contained in the directory and their association with a determined person.

A service provider may offer all or some of these services.

57. The policy statement of a certification or directory service provider must specify at least

(1) the information that may be entered in a certificate or directory and the information whose accuracy is confirmed, and the guarantees of accuracy offered by the service provider;

(2) the intervals at which the information is reviewed and the updating procedure;

(3) the persons to whom a certificate may be issued or who may cause information to be entered on a certificate or in a directory;

(4) the limits on the use of certificates and directory entries, including a limit on the value of the transactions for which they may be used;

(5) the information used to determine, when a communication is made, if a certificate or the information that a service user has caused to be entered on a certificate or in a directory is valid, suspended, cancelled or stored;

(6) the manner of obtaining additional information, where it is available but not yet entered on the certificate or in the directory;

(7) the confidentiality policy for information received or communicated by the service provider;

(8) the tariff for the entry of information in a directory or the issue, management and use of a certificate, and in particular the charge payable by certain classes of persons determined by government regulation;

(9) the process for dealing with complaints;

(10) the manner in which the service provider will dispose of certificates upon ceasing to operate or becoming bankrupt.

The policy statement of a certification or directory service provider must be accessible to the public.

58. A certification service provider may join a voluntary accreditation scheme. Accreditation shall be granted by a person or body designated by the Government. The terms and conditions for the granting of accreditation, the time within which accreditation is granted, the modification of accreditation conditions, the renewal, suspension or cancellation of accreditation, and the related fees, shall be established by government regulation.

The same criteria are applicable regardless of the territory of origin of the service provider. The certificates issued by an accredited service provider are deemed to meet the requirements of this Act.

59. The certificates issued by a certification service provider on the basis of standards other than those applicable in Québec may be considered to be equivalent to the certificates issued by an accredited certification service provider. The equivalency must be recognized by the person or body designated by the Government for the purposes of the conclusion of mutual recognition agreements for such certificates with the designated authority that established the standards. The same applies to directory services.

Accredited service providers, or service providers whose services are recognized as equivalent to those provided by an accredited service provider, must be entered in a register accessible to the public kept by the person or body that recognized the equivalency.

60. When an accreditation is issued or renewed, the following elements shall be taken into account in addition to the proposed policy statement:

(1) the fact that the applicant's identity is established;

(2) the scope of the expertise, the existing infrastructure, the services offered and the availability of financial guarantees to exercise the activity;

(3) the guarantees provided as to the independence and probity of the certification service provider and the policy established by the service provider to guarantee the expertise and probity of the persons dispensing the services;

(4) the guarantees of directory and certificate integrity, accessibility and security provided by the service provider;

(5) the applicability of the stated policies and, in the case of a renewal, of their application, and the fulfilment of the other obligations of the service provider.

61. A provider of certification services must present guarantees of impartiality concerning the person or object covered by the certification, even if the service provider is not a third party.

The service provider must ensure the reliability of the certificates issued during their entire life cycle, including when a certificate is modified, suspended, cancelled or stored and when the information it contains is updated.

62. Where certification applies to the holder of a key pair in an asymmetric encryption system, the person generating a key pair allowing a document to be signed must give the holder of the key pair the private key so that only that holder receives the secret information it contains.

The holder of the key pair must then ensure the confidentiality of the private key and every use of the private key is presumed to be made by the holder of the key pair, even if, in the case of a legal person, of a partnership or association or of the State, the holder of the key pair has authorized another person to hold the private key.

Where a private key is lost or stolen, or where the holder of the key pair or holder of the private key has reasonable grounds to believe that the private key's confidentiality is compromized, the certification service provider must be advised as soon as possible to allow the service provider to suspend or cancel the certificate for the public key. The holder of a private key who is not the holder of the certificate must advise the holder of the key pair.

No person may use a private key to sign a document after learning that the certificate issued for the corresponding public key has been suspended or cancelled.

63. A person who provides information in order to obtain a certificate is bound to inform the certification service provider, as soon as possible, of any change affecting the information.

Where the information is provided under a mandate or contract for services or of enterprise, the certificate holder is bound by the same requirement to provide information to the service provider.

64. When a technological document is used in a communication, the validity and scope of the certificate must be verified before the certificate is relied upon to obtain confirmation of the identity of any party to the communication or the accuracy of the identifier of an object.

Similarly, before the information contained in the certificate is relied upon, it is necessary to verify whether the certification service provider confirms the accuracy of the information.

The verification may be made in the directory or at the place indicated in the directory or with the service provider by means of a device for consultation on the premises or by remote access.

65. Certification and directory service providers and the persons referred to in sections 62 to 64 are bound only by an obligation of diligence.

Unless they can be relieved from liability, they are jointly liable to repair any damage resulting from a communication because of the inaccuracy or invalidity of a certificate or of the information contained in a directory. However, if there is no fault on their part, the reparation is shared equally among them.

No person may refuse to assume responsibility under this section.

66. The issue of a document as a certificate confirming the identity of a person or the accuracy of an object identifier, where no verification has been made by or for the service provider or where the verification carried out was so insufficient as to constitute an absence of verification, is false representation.

CHAPTER IV

HARMONIZATION OF SYSTEMS AND STANDARDS

67. The Government may form a multidisciplinary committee to promote the harmonization of the systems, norms and technical standards established for the purposes of this Act, with members, including a president, chosen by the Government after consultation with the business community, the information technology industry, the world of scientific and technical research and representatives of the public and parapublic sectors.

The president must be a member of the Bureau de normalisation du Québec. The committee may also receive assistance from persons having expertise relating to the field of information technology.

The members of the committee shall receive no remuneration, except in the cases, on the conditions and to the extent determined by the Government. They are, however, entitled to the reimbursement of the expenses incurred in the performance of their duties, on the conditions and to the extent determined by the Government.

68. The mission of the committee is to recommend ways which may

(1) ensure the compatibility or interoperability of media and technologies, and norms and standards for the production and signature of technological documents and their use in communications;

(2) avert the multiplication of processes, in particular as regards the verification of personal identity;

(3) promote the standardization of certificates and directories and the mutual recognition of certificates;

(4) guarantee the reliability of a technological document through security measures that are adequate to ensure its integrity during its entire life cycle;

(5) establish uniform auditing rules and practices, including the examination and evaluation of access, maintenance and backup methods, physical, logical and operational security measures, security registers and the correctives to be made in the event of a deficiency in an element that may affect the integrity of a document.

The committee is responsible for recommending criteria for the selection and use of formats and mark-up language, character representation codes, signature algorithms, encryption methods, data compression, image and audio enhancement, key length, and communications protocols or links.

The recommendations of the committee shall be forwarded to the minister responsible for the application of provisions relating to the implementation and development of information technologies.

Where the Government selects a process, system or technology, its selection shall reflect the recommendations and be published in the *Gazette officielle du Québec*. The selection must be made for a specific period; it may be extended, or a new selection may be made before or upon the expiry of the determined period. However, any new selection must be made taking into account the retention period of the documents based on the previous selections made and the need to continue to have access to those documents during their retention period.

69. Where this Act requires processes to be recognized by a national or international standards agency, or to be based on technical norms or standards for a medium that are recognized by such an agency for a specific purpose, the norms and standards may be those recognized by, among others, the Bureau de normalisation du Québec, the Standards Council of Canada, the Internet Engineering Task Force, the World Wide Web Consortium, the International Organization for Standardization or the International Telecommunication Union.

CHAPTER V

INTERPRETATION, AMENDING AND FINAL PROVISIONS

70. The concept of document, as used in this Act, applies to all documents referred to in legislative texts whether under the name document or under names such as act, annal, schedule, directory, order in council, ticket, directory,

licence, bulletin, notebook, map, catalogue, certificate, charter, statement of offence, decree, leaflet, drawing, diagram, writing, electrocardiogram, audio, video or electronic recording, bill, sheet, film, form, graph, guide, illustration, printed matter, newspaper, book, booklet, program, manuscript, model, microfiche, microfilm, note, notice, pamphlet, parchment, papers, photograph, minute, programme, prospectus, report, offence report and manual.

In this Act, the rules relating to documents may, depending on context, apply to an excerpt from a document or to a set of documents.

A record may comprise one or more documents.

71. Subparagraph 1 of the first paragraph of section 11 applies where the terms “duplicate”, “copy” and “original copy” are used in a legislative text in a context that indicates that the document to which they refer must be an original when used as the primary source for a reproduction.

72. Section 14 applies to technological documents where the term “certified copy”, “certified true copy” or “authentic copy” is used in a legislative text, and where the term “copy, “duplicate” or “triplicate” is used to refer to the obtention of a copy.

73. A reference, in an Act, to a specific means of delivery such as delivery by mail, by letter, by post, by messenger, by cablegram or telegram, by fax, by telematic, computerized or electronic means, using telecommunication, teletransmission, fibre optics or another information technology, whether in an open or closed communication network, does not preclude the use of another means of delivery appropriate to the medium of the document, as provided for in section 31.

74. Where an Act provides that a signature may be engraved or printed or affixed by means of an engraved, printed or lithographed facsimile, or that a mark may be made by means of a signature stamp, device or mechanical or automatic process, it shall be construed as allowing a signature to be made otherwise than by hand on a paper document, or as allowing a personal mark to be made by someone else. Such a provision shall not preclude the use of another mode of signature appropriate to the document where it is not a paper document.

75. A provision creating an offence that specifies that the offence may be committed using a document shall be construed as meaning that the offence is committed regardless of the fact that the document is on paper or another medium at any point in its life cycle.

76. Section VI of Chapter I of Title II of Book VII of the Civil Code of Québec (1991, chapter 64) is replaced by the following section:

“SECTION VI

“INTERCHANGEABILITY OF MEDIA

“2837. A writing can be used to adduce proof whatever its medium. However, where the medium involves the use of information technologies, the probative force of the writing is assessed pursuant to the Act respecting the legal normalization of new information technologies.”

77. Articles 2840 to 2842 of the said Code are replaced by the following articles:

“2840. The reproduction of a document in the possession of the State or of a legal person established in the public interest or for a private interest, in order to keep permanent proof of the document, must be authorized by a person in authority or the person responsible for document retention within the legal person or the State.

The person must, within a reasonable time, issue a statement attesting that authorization to reproduce the document has been given, describing the document to be reproduced and the reproductive process, setting out the place and date of reproduction and certifying that the two documents contain the same information. However, where reproduction occurs as part of a transfer of information to a medium based on another technology, a transfer declaration is sufficient if the purpose of reproduction is mentioned.

The reproduced document may be proved by filing a certified copy or the document resulting from the transfer.

“2841. The Act respecting the legal normalization of new information technologies applies to the reproduction of a document effected as part of a transfer or effected to obtain a copy of the document in a medium involving the use of information technologies.”

78. Article 2855 of the said Code is amended by adding the following sentence at the end: “However, where a material thing is a technological document, its admissibility as evidence is governed by the Act respecting the legal normalization of new information technologies.”

79. Article 2874 of the said Code is amended by replacing “reliable recording technique may be proved by such means, provided its authenticity is separately proved” by “recording technique may be proved by that means, provided it meets the standards of the Act respecting the legal normalization of new information technologies”.

80. Section 10 of the Act respecting Access to documents held by public bodies and the Protection of personal information (R.S.Q., chapter A-2.1) is amended by adding “or by remote access” at the end of the first paragraph.

81. Section 13 of the said Act is amended

(1) by replacing “can only be excercised” in the first paragraph by “is exercised”;

(2) by inserting “or by remote access” after “working hours” in the first paragraph;

(3) by inserting “or by remote access” after “working hours” in subsection 1 of the second paragraph.

82. Section 16 of the said Act is amended by replacing “shall not be exercised except by examining it on the premises during regular working hours” in the second paragraph by “is only exercised by examining it on the premises during working hours or by remote access”.

83. Section 84 of the said Act is amended by replacing “during regular working hours” in the first paragraph by “on the premises during regular working hours or by remote access”.

84. Section 2 of the Archives Act (R.S.Q., chapter A-21.1) is amended by striking out the definition of “document”.

85. The said Act is amended by inserting the following section after section 2:

“2.1. This Act does not apply to documents to which the Act respecting the Bibliothèque nationale du Québec (chapter B-2.1) applies.”

86. Section 31 of the said Act is replaced by the following section:

“31. Where the Keeper considers that a version of or excerpt from a document of a public body must be preserved permanently, he may require that it be reproduced for that purpose.”

87. Section 61 of the Code of Penal Procedure (R.S.Q., chapter C-25.1) is amended by adding, at the end, “and the Act respecting the legal normalization of new information technologies (*insert here the year and chapter number of this Act*)”.

88. Section 62.1 of the said Code is amended by striking out “, including the electronically-generated form,” in the first paragraph.

89. Sections 62.2 to 62.5, 67.1 and 68.1 of the said Code, enacted by sections 6, 10 and 11 of chapter 51 of the statutes of 1995, are repealed.

90. Section 71 of the said Code, amended by section 13 of chapter 51 of the statutes of 1995, is again amended

(1) by striking out ", including a digitized signature or a signature affixed by means of an automatic device," in the first paragraph;

(2) by striking out the second paragraph.

91. Section 184.1 of the said Code is amended by striking out "or in a document electronically joined to the statement of offence if the latter is drawn up electronically or digitized".

92. Section 191.1 of the said Code is amended

(1) by striking out "in electronic or hard copy form";

(2) by striking out "in such form".

93. Sections 218.1 and 225.1 of the said Code are repealed.

94. Section 367 of the said Code is amended

(1) by striking out ", including the electronically-generated form," in paragraph 1;

(2) by striking out paragraph 1.1.

95. Section 34 of the Real Estate Brokerage Act (R.S.Q., chapter C-73.1) is amended by inserting ", in paper form," after "contract" in the first paragraph.

96. Section 61 of the Interpretation Act (R.S.Q., chapter I-16) is amended by striking out paragraph 21.

97. Section 25 of the Consumer Protection Act (R.S.Q., chapter P-40.1) is amended by adding "and in paper form" at the end.

98. The Minister of Justice is responsible for the administration of the provisions of this Act relating to the legal aspect of information technologies, and the minister designated by the Government is responsible for the administration of the provisions relating to the implementation and development of information technologies.

99. The provisions of this Act come into force on the date or dates to be fixed by the Government.

TABLE OF CONTENTS