Updated to October 1 2021
This document has official status.

chapter C-1.1

ACT TO ESTABLISH A LEGAL FRAMEWORK FOR INFORMATION TECHNOLOGY

TABLE OF CONTENTS

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 media based on information technology, whether electronic, magnetic, optical, wireless or other, or based on a combination of technologies ;

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

(4) the linking of a person, an association, a partnership or the State with a technology-based document, by any means allowing them to be linked, such as a signature, or any means allowing them to be identified and, if need be, located, such as certification ; and

(5) concerted action for the harmonization of the technical systems, norms and standards involved in communications by means of technology-based documents and interoperability between different media and information technologies.

2001, c. 32, s. 1.

2. Except where a document is required by law to be in a specific medium or technology, any medium or technology may be used, provided the medium or technology chosen is in compliance with legal rules, in particular those contained in the Civil Code.

Hence, media used to inscribe documentary information are interchangeable and a requirement that a document be in writing does not entail the use of a specific medium or technology.

2001, c. 32, s. 2.

CHAPTER II

DOCUMENTS

DIVISION I

CONCEPT OF DOCUMENT

3. Information inscribed on a medium constitutes a document. The information is delimited and structured, according to the medium used, by tangible or logical features and is intelligible in the form of words, sounds or images. The information may be rendered using any type of writing, including a system of symbols that may be transcribed into words, sounds or images or another system of symbols.

For the purposes of this Act, a database whose structuring elements allow the creation of documents by delimiting and structuring the information contained in the database is considered to be a document.

A record may comprise one or more documents.

In this Act, a technology-based document is a document in any medium based on any information technology referred to in paragraph 2 of section 1.

2001, c. 32, s. 3.

4. A technology-based document, even when the information it contains is fragmented and dispersed in one or more media at one or more locations, is considered to form a whole if its logical structuring elements allow the fragments to be connected, directly or by reference, and if such elements ensure both the integrity of each fragment and the integrity of the document reconstituted as it existed prior to its fragmentation and dispersal.

Conversely, separate technology-based documents, even when combined into a single document for transmission or retention purposes, do not lose their distinct nature, if logical structuring elements ensure both the integrity of the combined document and the integrity of each separate reconstituted document.

2001, c. 32, s. 4.

DIVISION II

LEGAL VALUE AND INTEGRITY OF DOCUMENTS

5. The legal value of a document, particularly its capacity to produce legal effects and its admissibility as evidence, is neither increased nor diminished solely because of the medium or technology chosen.

A document whose integrity is ensured has the same legal value whether it is a paper document or a document in any other medium, insofar as, in the case of a technology-based document, it otherwise complies with the legal rules applicable to paper documents.

A document in a medium or based on technology that does not allow its integrity to be confirmed or denied may, depending on the circumstances, be admissible as testimonial evidence or real evidence and serve as commencement of proof, as provided for in article 2865 of the Civil Code.

Where the law requires the use of a document, the requirement may be met by a technology-based document whose integrity is ensured.

2001, c. 32, s. 5.

6. The integrity of a document is ensured if it is possible to verify that the information it contains has not been altered and has been maintained in its entirety, and that the medium used provides stability and the required perennity to the information.

The integrity of a document must be maintained throughout its life cycle, from creation, in the course of transfer, consultation and transmission, during retention and until archiving or destruction.

To assess the integrity of a document, particular account must be taken of the security measures applied to protect the document throughout its life cycle.

2001, c. 32, s. 6.

7. It is not necessary to prove that the medium of a document or that the processes, systems or technology used to communicate by means of a document ensure its integrity, unless the person contesting the admission of the document establishes, upon a preponderance of evidence, that the integrity of the document has been affected.

2001, c. 32, s. 7.

8. The Government may, on the basis of technical norms or standards approved by a recognized body referred to in section 68, make an order prescribing that a device is capable of fulfilling a determined function.

Where a device, its function and the norm or standard used are specified in such an order, it is not necessary to prove that the device is capable of fulfilling the function.

2001, c. 32, s. 8.

DIVISION III

EQUIVALENCE OF DOCUMENTS USED FOR THE SAME FUNCTIONS

9. Two or more documents in different media have the same legal value if they contain the same information, if the integrity of each document is ensured and if each document complies with the applicable legal rules. One document may be substituted for another and the documents may be used simultaneously or in alternation. In addition, all such documents may be used for the same purposes.

If a document is lost, another document may serve to reconstitute it.

2001, c. 32, s. 9.

10. The sole fact that documents containing the same information but in different media show differences in the way in which the information is stored or presented, or contain different information, whether visible or hidden, relating to the medium used or to security, shall not be considered as affecting 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 shall not be considered as affecting the integrity of the documents.

2001, c. 32, s. 10.

11. In the event of a divergence between documents in different media or based on different technologies that purport to contain the same information, the document containing information that can be verified as being unaltered and maintained in its entirety shall prevail unless evidence to the contrary is adduced.

2001, c. 32, s. 11.

12. A technology-based document may fulfil the functions of an original. To that end, the integrity of the document must be ensured and, where the desired function is to establish

(1) that the document is the source document from which copies are made, the components of the source document must be retained so that they may subsequently be used as a reference ;

(2) that the document is unique, its components or its medium must be structured by a process that makes it possible to verify 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) that the document is the first form of a document linked to a person, its components or its medium must be structured by a process that makes it possible to verify that the document is unique, to identify the person with whom the document is linked and to maintain the link throughout the life cycle of the document.

For the purposes of subparagraphs 2 and 3 of the first paragraph, the processes must be based on technical norms and standards approved by a recognized body referred to in section 68.

2001, c. 32, s. 12.

13. Where the function of affixing a seal, signet, press, stamp or other instrument is

(1) to preserve the integrity of a document or authenticate the document as an original, the purpose may be achieved, in the case of a technology-based document, by means of any process appropriate to the medium used ;

(2) to identify a person, an association, a partnership or the State, the purpose may be achieved, in the case of a technology-based document, according to the rules provided in subdivision 1 of Division II of Chapter III ;

(3) to protect the confidentiality of a document, the purpose may be achieved in the case of a technology-based document, according to the rules provided in section 34.

2001, c. 32, s. 13.

14. As regards the form of a document, one or more processes may be used to fulfil the functions or achieve the purposes provided for in sections 12 and 13, making use of the characteristic features of the medium used.

2001, c. 32, s. 14.

15. To ensure the integrity of a copy of a technology-based document, the copying process must offer a sufficient guarantee that it contains the same information as the source document.

To assess the integrity of a copy, account must be taken of the circumstances in which the copy was made and of whether it was made systematically and without interruption or by means of a process meeting the technical norms or standards approved by a recognized body referred to in section 68.

However, where it is necessary to establish that a document is a copy, it must include characteristics as to form allowing it to be recognized as 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 characteristic.

The integrity of a copy generated by an enterprise within the meaning of the Civil Code or by the State shall be presumed in favour of third persons.

2001, c. 32, s. 15.

16. Where a copy of a technology-based document must be certified, the requirement may be met by means of a comparison process that verifies that the information in the copy is identical to the information in the source document.

2001, c. 32, s. 16.

DIVISION IV

MAINTENANCE OF INTEGRITY OF DOCUMENTS THROUGHOUT LIFE CYCLE

§ 1. — *Transfer of information*

17. The information contained in an original document or a copy that must be retained for evidential purposes may be transferred to another medium based on a different technology.

However, subject to section 20, in order for the source document to be destroyed and replaced by the document resulting from the transfer without compromising legal value, the transfer must be documented so that it may be shown, if need be, that the resulting document contains the same information as the source document and that its integrity is ensured.

Transfer documentation must include a reference to the original format of the source document, the transfer process used and the guarantees it purports to offer, according to the specifications provided with the

product, as regards the integrity of the source document, if it is not destroyed, and the integrity of the resulting document.

The documentation, including that pertaining to any previous transfer, must be retained throughout the life cycle of the resulting document. The documentation may be attached, directly or by reference, to the resulting document, to its structuring elements or to the medium.

2001, c. 32, s. 17.

18. If the source document is destroyed, no rules of evidence may be invoked against the admissibility of a document resulting from a transfer effected and documented in conformity with section 17 to which the documentation referred to in that section is attached, on the sole ground that the document is not in its original form.

2001, c. 32, s. 18.

§ 2. — *Retention of documents*

19. Every person must, during the period a document is required to be retained, ensure that its integrity is maintained and see to it that equipment is available to make the document accessible and intelligible and usable for the purposes for which it is intended.

2001, c. 32, s. 19.

20. Documents that are required by law to be retained and that have been transferred may be destroyed and replaced by the documents resulting from the transfer. However, before such documents may be destroyed, the person responsible must

(1) unless the person is an individual, establish and update rules to be applied prior to the destruction for transferred documents ;

(2) make sure that any confidential personal information contained in the documents to be destroyed is protected ; and

(3) make sure that the documents, if 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 (chapter A-21.1).

However, a document which, in its original medium, has archival, historical or heritage value according to the criteria established under paragraph 1 of section 69 must be preserved in its original medium even if it has been transferred.

2001, c. 32, s. 20.

21. If a technology-based document is modified during its retention period, the person having the authority to make the modification must, in order to preserve the integrity of the document, record the name of the person having requested the modification, the time and reason for the modification and the name of the person having made the modification. The modification forms an integral part of the document even if it is recorded in a separate document.

2001, c. 32, s. 21.

22. A service provider, acting as an intermediary, that provides document storage services on a communication network is not responsible for the activities engaged in by a service user with the use of documents stored by the service user or at the service user’s request.

However, the service provider may incur responsibility, particularly 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 that provides technology-based documentary referral services, such as an index, hyperlinks, directories or search tools, is not responsible for activities engaged in by a user of such services. However, the service provider may incur responsibility, particularly 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 the persons known by the service provider to be engaging in such an activity.

2001, c. 32, s. 22.

§ 3. — *Consultation of documents*

23. Every document to which a person has a right of access must be intelligible, either directly or through the use of information technology.

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

The wishes of the person having the right of access as to the medium or technology to be used must be taken into account, unless substantial practical difficulties would be involved, owing in particular to high cost or the information transfer required.

2001, c. 32, s. 23.

24. The use of extensive search functions in a technology-based document containing personal information which is made public for a specific purpose must be restricted to that purpose. The person responsible for access to the document must see to it that appropriate technological means are in place to achieve that end. The person may also set conditions for the use of such search functions, in accordance with the criteria determined under paragraph 2 of section 69.

2001, c. 32, s. 24.

25. The person responsible for access to a technology-based document containing confidential information must take appropriate security measures to protect its confidentiality, such as controlling access to the document by means of a restricted view technique, or any technique that prevents unauthorized persons from accessing such information or from otherwise accessing the document or the components providing access to the document.

2001, c. 32, s. 25.

26. Anyone who places a technology-based document in the custody of a service provider is required to inform the service provider beforehand as to the privacy protection required by the document according to the confidentiality of the information it contains, and as to the persons who are authorized to access the document.

During the period the document is in the custody of the service provider, the service provider is required to see to it that the agreed technological means are in place to ensure its security and maintain its integrity and, if applicable, protect its confidentiality and prevent accessing by unauthorized persons. Similarly, the service provider must ensure compliance with any other obligation provided for by law as regards the retention of the document.

2001, c. 32, s. 26.

27. A service provider, acting as an intermediary, that provides communication network services or who stores or transmits technology-based documents on a communication network is not required to monitor the information communicated on the network or contained in the documents or to identify circumstances indicating that the documents are used for illicit activities.

However, the service provider 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, in accordance with the applicable legislative provisions, as regards public security or the prevention, detection, proof and prosecution of offences.

2001, c. 32, s. 27.

§ 4. — *Transmission of documents*

28. A document may be transmitted, sent or forwarded by any means appropriate to the medium, unless the exclusive use of a specific means of transmission is required by law.

Where the law requires the use of mail, the requirement may be met by means of the technology appropriate to the medium of the document. Similarly, where the law requires the use of registered mail, the requirement may be met, in the case of a technology-based document, by means of an acknowledgement of receipt in the appropriate medium signed by the recipient, or by any other agreed method.

Where the law requires the transmission or reception of a document at a specific address, the address shall comprise, in the case of a technology-based document, an identifier specific to the location where the recipient may receive communication of such document.

2001, c. 32, s. 28; I.N. 2016-01-01 (NCCP).

29. A person may not be required to acquire a specific medium or technology to transmit or receive a document, unless such requirement is expressly provided by law or by an agreement.

Similarly, no person may be required to receive a document in a medium other than paper, or by means of technology that is not at the person’s disposal.

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, at the option of the recipient of the product or service.

2001, c. 32, s. 29.

30. For the technology-based document received to have the same value as the document transmitted, the means of transmission must allow the integrity of both documents to be preserved. Documentation establishing the ability of a means of transmission to preserve the integrity of both documents must be available for production as evidence.

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 its integrity has been affected.

2001, c. 32, s. 30.

31. A technology-based document is presumed transmitted, sent or forwarded where the action required to send it to the active address of the recipient has been accomplished by or on the instructions of the sender, and the transmission cannot be stopped or, although it can be stopped, is not stopped by or on the instructions of the sender.

A technology-based document is presumed received or delivered where it becomes accessible at the address indicated by the recipient as the address where the recipient accepts the receipt of documents from the sender, or at the address that the recipient publicly represents as the address where the recipient accepts the receipt of documents, provided the address is active at the time of sending. The document received is presumed intelligible, unless notice to the contrary is sent to the sender as soon as the document is accessed.

The time of sending or of receipt of a document may be established by producing a transmission slip or an acknowledgement of receipt or the information kept with the document providing it guarantees the date, hour, minute and second of sending or receipt and indicates the source and destination of the document, or by any other agreed method that provides the same guarantees.

2001, c. 32, s. 31.

32. Where the law requires that two or more copies of a document be transmitted, sent, forwarded, remitted or delivered to one and the same recipient, the requirement may be met, in respect of a technology-based document transmittable on a communication network, by the transmission of a single copy.

2001, c. 32, s. 32.

33. A presumption of document integrity exists in favour of a third person who generates a copy of a document of an enterprise, within the meaning of the Civil Code, or a document in the State's possession by means of a system or from a document, including a program, placed at the person's disposal by the enterprise or the State.

2001, c. 32, s. 33.

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

Documentation explaining the agreed mode of transmission, including the means used to protect the confidentiality of the transmitted document, must be available for production as evidence.

2001, c. 32, s. 34.

35. A party that offers a product or service by means of a pre-programmed document must, on pain of non-enforceability of the communication or cancellation of the transaction, see to it that the document provides instructions that allow users to promptly advise the party of any errors or contains means that allow users to avoid or correct errors. Similarly, users must be provided instructions or means to avoid receiving unwanted products or services because of an ordering error, or instructions for the return or destruction of unwanted products.

2001, c. 32, s. 35.

36. A service provider, acting as an intermediary, that provides communication network services exclusively for the transmission of technology-based documents is not responsible for acts of service users performed with the use of the documents transmitted or stored during the normal course of the transmission for the time required for the efficiency of the transmission.

However, the service provider may incur responsibility, particularly if the service provider otherwise participates in acts performed by service users

(1) by being the sender of a document ;

(2) by selecting or altering the information in a document ;

(3) by determining who transmits, receives or has access to a document ; or

(4) by storing a document longer than is necessary for its transmission.

2001, c. 32, s. 36.

37. A service provider, acting as an intermediary, which, as part of transmission services provided via a communication network, maintains technology-based documents furnished by clients on that network for the sole purpose of ensuring the efficiency of their subsequent transmission to persons having a right to access the information, is not responsible for acts of service users performed with the use of those documents.

However, the service provider may incur responsibility, particularly if the service provider otherwise participates in acts performed by service users

(1) as specified in the second paragraph of section 36 ;

(2) by not complying with the conditions for access to a document ;

(3) by preventing the verification of who has accessed a document ;

(4) by failing to withdraw a document from the network or to block access to the document after becoming aware that the document has been withdrawn from its initial position on the network, that persons having the right to access the document are unable to do so or that a competent authority has ordered that the document be withdrawn from the network or that access to the document be blocked.

2001, c. 32, s. 37.

CHAPTER III

ESTABLISHMENT OF LINK WITH TECHNOLOGY-BASED DOCUMENTS

DIVISION I

CHOOSING A LINKING PROCESS

38. The link between a person and a technology-based document, or the link between such a document and an association, a partnership or the State, may be established by any process or combination of processes, to the extent that it allows

(1) the identity of the person or the identification of the association, partnership or the State and, where applicable, their location, to be confirmed, and allows their link with the document to be confirmed ; and

(2) the document to be identified and, if need be, allows its origin and destination at any given time to be determined.

2001, c. 32, s. 38.

39. The link between a person and a document, whatever the medium used, may be established by means of the person’s signature. A person’s signature may be affixed to the document by means of any process that meets the requirements of article 2827 of the Civil Code.

A person’s signature affixed to a technology-based document may be set up against that person if the integrity of the document is ensured and the link between the signature and the document was established at the time of signing and has since been maintained.

2001, c. 32, s. 39.

DIVISION II

MODES OF IDENTIFICATION AND LOCATION

§ 1. — *Persons, associations, partnerships or the State*

40. A person who, following verification, is able to confirm the identity of a person or the identification of an association, a partnership or the State may do so by means of any document, such as a certificate, whose integrity is ensured. The document may be transmitted in any medium provided confidential information is protected.

A person's identity or an entity's identification must be verified in compliance with the law. It may be verified by reference to the registers kept pursuant to the Civil Code or the Act respecting the legal publicity of enterprises (chapter P-44.1), regardless of the medium used to communicate. A person's identity may also be verified on the basis of the person's characteristics or knowledge of certain facts 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 documents whose integrity is ensured as may be available in different media for consultation on the premises or by remote access.

2001, c. 32, s. 40; 2010, c. 7, s. 282.

41. The use, as proof of one's identity or the identity of another person, of a technology-based document specifying a personal characteristic or a particular fact or indicating that the person to be identified possesses a particular object requires that the integrity of the document be preserved.

Such a document must, in addition, be protected from interception if its storage or transmission on 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.

2001, c. 32, s. 41.

42. Where an attestation, card, certificate, identity document or other document is required by law to identify a person, the requirement may be met by means of a technology-based document in a medium appropriate to the medium of the document.

2001, c. 32, s. 42.

43. A person may not be required to submit, for identification purposes, to a process or device that affects the person's physical integrity.

Unless otherwise expressly provided by law for health protection or public security reasons, a person may not be required to be connected to a device that allows the person's whereabouts to be known.

2001, c. 32, s. 43.

44. A person's identity may not be verified or confirmed by means of a process that allows biometric characteristics or measurements to be recorded, except with the express consent of the person concerned. Where consent is obtained, only the minimum number of characteristics or measurements needed to link the person to an act and only such characteristics or measurements as may not be recorded without the person's knowledge may be recorded for identification purposes.

No other information revealed by the characteristics or measurements recorded may be used as a basis for a decision concerning the person or for any other purpose whatsoever. Such information may only be disclosed to the person concerned, at the person's request.

The record of the characteristics or measurements and any notation relating thereto must be destroyed as soon as the purpose of verification or confirmation of identity has been met or the reason for the verification or confirmation no longer exists.

2001, c. 32, s. 44.

45. The creation of a database of biometric characteristics and measurements must be disclosed beforehand to the Commission d'accès à l'information. As well, the existence of such a database, whether or not it is in service, must be disclosed to the Commission.

The Commission may make orders determining how such databases are to be set up, used, consulted, released and retained, and how measurements or characteristics recorded for personal identification purposes are to be archived or destroyed.

The Commission may also suspend or prohibit the bringing into service or order the destruction of such a database, if the database is not in compliance with the orders of the Commission or otherwise constitutes an invasion of privacy.

2001, c. 32, s. 45.

§ 2. — *Documents and other objects*

46. Where a document used for a network communication must be retained for evidential purposes, the person responsible for the document must store the identifier of the document with the document throughout its life cycle.

The identifier of the document must be accessible through a directory service, capable of linking an identifier with its location. The link 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.

The identifier shall comprise a reference name that is unique and unambiguous within the set of local names where it is registered, along with the necessary extensions to link the name to sets of universal names.

To allow the origin or destination of a document at any given time to be established, the other objects used to transmit the document, such as certificates, algorithms and originating and receiving servers, must be identifiable and locatable by means of the identifiers assigned to each.

2001, c. 32, s. 46.

DIVISION III

CERTIFICATION

§ 1. — *Certificates and directories*

47. A certificate may be used to establish one or more facts including the confirmation of a person's identity, the identification of a partnership, an association or the State, the correctness of the identifier of a document or other object, the attributes of a person, document or other object or the link between a document or other object and a tangible or logical identification or location device.

An attribute certificate may be used to certify a person's function, capacity, rights, and powers or privileges within a legal person, association, partnership or the State or within a position of employment. An attribute certificate may be used to certify the location of an association, or partnership or of a location where the State sends or receives documents. An attribute certificate may also be used to confirm the information used to identify or locate a document or object or determine the use of or the right of access to a document or object or any other right or privilege relating to a document or object.

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

2001, c. 32, s. 47.

48. A certificate may be attached 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 contain, at least, the following information :

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

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

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

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

(5) in the case of a certificate confirming the identity of a person or the identification of an association, a partnership or the State, the distinctive name of the person or entity or, in the case of a certificate confirming the identifier of an object, that identifier ; and

(6) in the case of an attribute certificate, the designation of the attribute confirmed by the certificate and, if need be, the identification of the person, association, partnership, State or object to which it is linked.

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

2001, c. 32, s. 48.

49. Where a legal person, an association, a partnership or the State acts through an authorized natural person, the certificate confirming its identification must indicate who is acting. Failing such indication, the natural person must attach one or more certificates confirming such fact.

2001, c. 32, s. 49.

50. A directory whose function is to identify or locate a person or object, to confirm the identification of or locate an association, a partnership or the State, to locate a place where the State sends or receives documents, or to establish a link between any such entity and an object, must be constituted in accordance with the technical norms or standards approved by a recognized body referred to in section 68.

The directory must be accessible to the public, either directly or by means of a device for consultation on the premises or by remote access, or by means of a procedure or through an intermediary, that can access various domains of a network where confirmation of the validity of an identifier, a certificate or any other information included in the directory may be obtained.

However, the reason for the suspension or cancellation of a certificate is accessible only on the authorization of the person having suspended or cancelled it.

2001, c. 32, s. 50.

§ 2. — *Certification and directory services*

51. Certification and directory services may be provided by a person or by the State.

Certification services involve verifying the identity of persons and issuing certificates confirming personal identity, the identification of an association, a partnership or the State or the correctness of an object identifier. 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 link with the information they confirm.

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

2001, c. 32, s. 51.

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

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

(2) the information review intervals and the updating procedure ;

(3) who may be issued a certificate and who may cause information to be entered in a certificate or a directory ;

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

(5) how it can be determined, upon making a communication, whether a certificate or information entered in a certificate or in a directory is valid, suspended, cancelled or stored ;

(6) how additional available information not yet entered in the certificate or the directory, especially as regards updated use restrictions applicable to certificates, may be obtained ;

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

(8) the complaints procedure ; and

(9) how certificates will be disposed of by the service provider upon ceasing to operate or becoming bankrupt.

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

2001, c. 32, s. 52.

53. A certification service provider may join a voluntary accreditation scheme. Accreditation shall be granted, subject to satisfaction of the requirements of paragraph 3 of section 69, by a person or body designated by the Government.

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

2001, c. 32, s. 53.

54. 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 certificates issued by an accredited certification service provider. Their equivalency must be recognized by the person or body designated by the Government for the purpose of concluding mutual recognition agreements with the designated authority having established the standards. The same applies to directory services.

A public register of all accredited service providers, or service providers whose services are recognized as equivalent to those provided by an accredited service provider, shall be kept by the accrediting person or body or by the person or body that recognizes equivalency.

2001, c. 32, s. 54.

55. To decide whether an accreditation may be granted or renewed, account must be taken of the information contained in the proposed policy statement and at least of

(1) whether the applicant's identity has been established ;

(2) the extent of the applicant's expertise, the existing infrastructure, the services offered and the regularity and extent of audits ;

(3) the availability of financial guarantees for the proposed activity ;

(4) the guarantees offered as to the independence and probity of the applicant and the policy established by the applicant to guarantee the expertise and probity of the persons dispensing the services ;

(5) the guarantees offered as to directory or certificate integrity, accessibility and security ; and

(6) the applicability of the stated policies and, in the case of a renewal, the implementation of the policies, and the fulfilment of the other obligations of a service provider.

2001, c. 32, s. 55.

56. A certification service provider must offer guarantees of impartiality towards any person or object that is the subject of a certification, even if the service provider is not a third person in relation to the person or object.

The service provider must ensure the integrity of certificates throughout their life cycle, including when they are modified, suspended, cancelled or archived and when the information they contain is updated.

In addition, the service provider must be able to confirm the link between the tangible or logical identification or location device and the person, association, partnership, State or object identified or located by means of the device.

The issue of a document represented to be a certificate confirming the identity of a person, the identification of an association, a partnership or the State or the correctness of an object identifier, where no verification has been carried out by or for the service provider or where the verification was so insufficient as to constitute an absence of verification, is false representation.

2001, c. 32, s. 56.

57. Where the certification applies to the holder of a tangible or logical device that allows the holder to be identified or located or one of the holder's attributes to be specified and where the device contains a secret element, the holder must protect its confidentiality. Where the secret element must be transmitted to the holder of the device, the transmission must be done in such a manner that only the holder of the device is informed thereof.

The holder of the device must see to it that the device is not used without authorization. Every use of the device is presumed to be made by the holder of the device.

2001, c. 32, s. 57.

58. The holder of a device who has reasonable grounds to believe that the device has been stolen or lost or that its confidentiality is at risk must, as soon as practicable, advise

(1) any person the holder has authorized to use the device ;

(2) any third person who may reasonably be expected to act on the basis of the fact that the device was used by a person authorized to use it ; and

(3) the certification service provider so that the certificate linked to the device may be suspended or cancelled.

An authorized person is bound by the same obligation to advise the holder of the device and the persons referred to in subparagraphs 2 and 3.

No person may use a tangible or logical device to sign a document after learning that the certificate issued for the device has been suspended or cancelled.

2001, c. 32, s. 58.

59. A person who provides information in order to be issued a certificate is bound to inform the certification service provider, as soon as practicable, of any change affecting the information.

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

2001, c. 32, s. 59.

60. When a technology-based document is to be used in a communication, the validity and scope of the certificate must be verified before the certificate may be relied upon, in order to obtain confirmation of the identity or identification of any party to the communication or of the correctness of an object identifier.

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

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.

2001, c. 32, s. 60.

61. The certification and directory service providers, the holder of a certificate and any person who relies on a certificate to act are, in respect of their obligations under this Act, bound by an obligation of diligence.

2001, c. 32, s. 61.

62. Where a transaction is carried out by means of a technology-based document supported by a certificate appropriate to the transaction, in accordance with subparagraphs 4 and 6 of the first paragraph of section 52, each of the persons referred to in section 61 is liable for any damage resulting from the inaccuracy or invalidity of the certificate or of any information contained in the directory, unless the person shows that he or she has committed no fault in the performance of his or her obligations. Where two or more of them are liable, the obligation to provide reparation for the damage is a joint obligation ; if liability cannot be apportioned, it is apportioned equally among them. In addition, if there is no fault on the part of any of those persons, reparation for the damage shall be provided by them jointly and equally.

None of those persons may refuse to assume liability under this section.

2001, c. 32, s. 62.

CHAPTER IV

ESTABLISHMENT OF TECHNOLOGICAL AND LEGAL INFRASTRUCTURES

DIVISION I

HARMONIZATION OF TECHNICAL SYSTEMS, NORMS AND STANDARDS

63. A multidisciplinary committee shall be formed to promote the harmonization, both at the national and international levels, of the technical processes, systems, norms and standards established for the purposes of this Act. To that end, the Government shall, after consultation with the Bureau de normalisation du Québec, call upon persons from the business community, the information technology industry and the scientific and technical community, persons from the public, parapublic and municipal sectors and persons belonging to the professional orders, all of whom must have expertise in the field of information technology.

The committee shall be chaired by a representative of the Bureau de normalisation du Québec. The committee may call upon other persons having expertise in the field of information technology. The secretariat of the committee is the responsibility of the Bureau.

The members of the committee shall receive no remuneration, except in such cases, on such conditions and to such extent as may be determined by the Government. They are, however, entitled to the reimbursement of expenses incurred in the exercise of their functions, on the conditions and to the extent determined by the Government.

2001, c. 32, s. 63.

64. The mission of the harmonization committee is to examine ways to

(1) ensure the compatibility of or interoperability between different media and technologies, and the harmonization of technical norms and standards for the production and signature of technology-based 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 integrity of technology-based documents through physical, logical or operational security measures and document management measures capable of ensuring the integrity of documents throughout their life cycle ;

(5) standardize auditing practices, including the examination and evaluation of accessing, maintenance and backup methods, physical, logical and operational security measures, security registers and correctives in the event of a deficiency that may affect the integrity of documents ; and

(6) facilitate the application of this Act, making appropriate recommendations.

2001, c. 32, s. 64.

65. The committee shall develop practical guidelines reflecting the consensus reached on the subjects referred to in section 64.

The guidelines shall determine the common technical standards selected, such as 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 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, the guidelines must specify that any new selection must provide for the

retention period of documents based on the previous selections and the need for continued access to those documents throughout their retention period.

The guidelines shall be published and updated by the Bureau de normalisation du Québec.

2001, c. 32, s. 65.

66. The Bureau shall report annually to the Minister on the proceedings of the harmonization committee and on the voluntary implementation of the guidelines.

Within 30 days after receiving the report, the Minister shall forward a copy to the Government and shall lay the report before the National Assembly within the next 30 days or, if the Assembly is not in session, within 30 days of resumption.

2001, c. 32, s. 66.

67. If the guidelines are not implemented voluntarily in whole or in part, the Government may, after consultation with the committee, substitute regulatory provisions for the guidelines.

2001, c. 32, s. 67.

68. Where this Act requires that a technical process, norm or standard be approved by a recognized body to establish that it is capable of fulfilling a specific function, the recognition may be given by

(1) the International Electrotechnical Commission (IEC), the International Organization for Standardization (ISO) or the International Telecommunication Union (ITU) ;

(2) the Standards Council of Canada or a body accredited by that Council ; or

(3) the Bureau de normalisation du Québec.

The recognition may include a reference to a process or documentation developed by an experts group, such as the Internet Engineering Task Force or the World Wide Web Consortium.

2001, c. 32, s. 68.

DIVISION II

REGULATORY POWERS OF THE GOVERNMENT

69. In addition to such substitute standards as may be prescribed under section 67, the Government may make regulations determining

(1) criteria for the recognition of the archival, historical or heritage value of a document in its original medium ;

(2) criteria for the use of extensive search functions in respect of personal information contained in technology-based documents that are made public for a specific purpose ;

(3) the accreditation procedure applicable to certification service providers, the requirements and waiting period for accreditation and for a modification of accreditation conditions, the requirements for accreditation renewal and the conditions that can lead to the suspension or cancellation of accreditation, and the related fees ; and

(4) so as to ensure the security of documentary communications and if the Government is of the opinion that it is required in the public interest, the cases warranting and the conditions applicable to the use of a specific medium or technology.

2001, c. 32, s. 69.

CHAPTER V

INTERPRETATION AND AMENDING AND FINAL PROVISIONS

70. No provision of this Act shall be construed as limiting rights existing on 1 November 2001.

Similarly, no provision of this Act shall be construed as affecting the legal value of documentary communications effected before 1 November 2001.

2001, c. 32, s. 70.

71. The concept of document, as used in this Act, is applicable to all documents referred to in legislative texts whether by the term "document" or by terms such as act, deed, record, annals, schedule, directory, order, order in council, ticket, directory, licence, bulletin, notebook, map, catalogue, certificate, charter, cheque, 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, computer program, manuscript, model, microfiche, microfilm, note, notice, pamphlet, parchment, papers, photograph, minute, program, prospectus, report, offence report, manual and debt security or title of indebtedness.

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.

2001, c. 32, s. 71.

72. Subparagraph 1 of the first paragraph of section 12 applies where the terms "duplicate", "copy", "original copy" and "triplicate" are used in a legislative text in a context that indicates that the document to which they refer must fulfil the function of an original as the source document from which copies are made.

2001, c. 32, s. 72.

73. Section 16 applies to technology-based documents where the term "certified copy", "certified true copy" or "authentic copy" is used in a legislative text, and where the term "collate", "copy", "duplicate", "triplicate" or "authenticated" is used in connection with the issue of a copy.

2001, c. 32, s. 73.

74. A reference in the law to the possibility of using one or more specific means of transmission such as sending by mail, by messenger, by cablegram or telegram, by fax, by telematic, computerized or electronic means, by way of telecommunication, teletransmission, fibre optics or any other information technology, does not preclude the use of another means of transmission appropriate to the medium of the document to be sent, provided the legislative provision does not require the exclusive use of a specific means of transmission.

2001, c. 32, s. 74.

75. Where it is provided by law 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 affixed on a paper document otherwise than by hand, or as allowing a personal mark to be affixed on a paper document by

someone else. Such a provision does not preclude the use of another mode of signature appropriate to the document in a medium other than paper.

2001, c. 32, s. 75.

75.1. Where it is provided by law that a signature affixed to a document by the representative of a department or body referred to in section 3 of the Public Administration Act (chapter A-6.01) shall be done by means of a process authorized by law, in particular where the law provides that the signature requirements are determined by the Government or the Minister or the body, the signature may, in the absence of such authorization or such requirements, be affixed by means of any process that meets the requirements of article 2827 of the Civil Code.

2021, c. 22, s. 23.

76. A provision creating an offence that specifies that the offence may be committed with the use of a document shall be construed as meaning that an offence may be committed whatever the medium of the document may have been, whether paper or any other, at any point in its life cycle.

2001, c. 32, s. 76.

77. *(Omitted).*

2001, c. 32, s. 77.

78. *(Omitted).*

2001, c. 32, s. 78.

79. *(Omitted).*

2001, c. 32, s. 79.

80. *(Omitted).*

2001, c. 32, s. 80.

81. *(Omitted).*

2001, c. 32, s. 81.

82. *(Amendment integrated into c. A-2.1, s. 10).*

2001, c. 32, s. 82.

83. *(Amendment integrated into c. A-2.1, s. 13).*

2001, c. 32, s. 83.

84. *(Amendment integrated into c. A-2.1, s. 16).*

2001, c. 32, s. 84.

85. *(Amendment integrated into c. A-2.1, s. 84).*

2001, c. 32, s. 85.

86. *(Amendment integrated into c. A-21.1, s. 2).*

2001, c. 32, s. 86.

87. *(Amendment integrated into c. A-21.1, s. 2.1).*

2001, c. 32, s. 87.

88. *(Amendment integrated into c. A-21.1, s. 31).*

2001, c. 32, s. 88.

89. *(Amendment integrated into c. C-8.1, s. 16).*

2001, c. 32, s. 89.

90. *(Amendment integrated into c. C-25, a. 89).*

2001, c. 32, s. 90.

91. *(Amendment integrated into c. C-25.1, a. 61).*

2001, c. 32, s. 91.

92. *(Amendment integrated into c. C-25.1, a. 62.1).*

2001, c. 32, s. 92.

93. *(Omitted).*

2001, c. 32, s. 93.

94. *(Amendment integrated into c. C-25.1, a. 71).*

2001, c. 32, s. 94.

95. *(Amendment integrated into c. C-25.1, a. 184.1).*

2001, c. 32, s. 95.

96. *(Amendment integrated into c. C-25.1, a. 191.1).*

2001, c. 32, s. 96.

97. *(Omitted).*

2001, c. 32, s. 97.

98. *(Amendment integrated into c. C-25.1, a. 367).*

2001, c. 32, s. 98.

99. *(Amendment integrated into c. C-73.1, s. 34).*

2001, c. 32, s. 99.

100. *(Amendment integrated into c. I-16, s. 61).*

2001, c. 32, s. 100.

101. *(Amendment integrated into c. P-40.1, s. 25).*

2001, c. 32, s. 101.

102. *(Amendment integrated into c. P-40.1, s. 127).*

2001, c. 32, s. 102.

103. *(Amendment integrated into c. R-2.2, s. 34).*

2001, c. 32, s. 103.

104. The minister responsible for the administration of this Act shall be designated by the Government.

2001, c. 32, s. 104.

The Minister responsible for Government Administration and Chair of the Conseil du trésor is responsible for the administration of this Act except sections 5 to 16, 22, 27, 31, 33, 36, 37, 39, 61 and 62. Order in Council 658-2020 dated 22 June 2020, (2020) 152 G.O. 2 (French), 2936.

The Minister of Justice is responsible for the administration of sections 5 to 16, 22, 27, 31, 33, 36, 37, 39, 61 and 62 of this Act. Order in Council 656-2020 dated 22 June 2020, (2020) 152 G.O. 2 (French), 2935.

105. *(Omitted).*

2001, c. 32, s. 105.

REPEAL SCHEDULE

In accordance with section 9 of the Act respecting the consolidation of the statutes and regulations (chapter R-3), chapter 32 of the statutes of 2001, in force on 1 April 2002, is repealed, except sections 77 to 81 and 105, effective from the coming into force of chapter C-1.1 of the Revised Statutes.