Draft Regulation

Civil Code of Québec
(1991, c. 64)

An Act respecting the implementation of the reform of the Civil Code
(1992, c. 57)

An Act respecting registry offices
(R.S.Q., c. B-9)

Register of personal and movable real rights — Amendments

Notice is hereby given, in accordance with sections 10 and 11 of the Regulations Act (R.S.Q., c. R-18.1), that the Regulation to amend the Regulation respecting the register of personal and movable real rights, the text of which appears below, may be made by the Government at the expiry of 45 days following this publication.

The purpose of the draft Regulation is to establish a secure infrastructure for the electronic transmission of data between the registry office and its clients, and for the processing and storage of that data.

Therefore, the draft Regulation proposes to amend the provisions relating to the medium, the form and the signing of an application for registration in order to take into account the fact that it may be transmitted in paper form or in electronic form. It introduces new requirements relating to the issuing of copies of applications for registration transmitted electronically as well as to the storage on microfilm or on an optical medium of the applications for registration submitted on paper or electronically.

Studies to date have revealed no impact on the public. However, the draft Regulation will have the following effects on business:

— clients will be able to transmit their applications for registration quickly and efficiently from anywhere in the province, thereby accelerating the publication of rights contained in the register of personal and movable real rights;

— it will improve the reliability of the entries made in the register since it provides for the verification of the identity and signature of the sender and safeguards the integrity and completeness of the transmitted messages in addition to eliminating possible data entry errors in the processing of applications by the registrar; and

— it will facilitate the implementation of the second phase of the register in that it provides for the registration of reservations of ownership following instalment sales, rights of ownership of lessors, and movable hypothecs without delivery on consumer goods.

Further information may be obtained from Ms. Lise Cadoret, notary, at 255, boulevard Crémazie Est, 5e étage, Montréal (Québec) H2M 2V3; telephone (514) 864-4931; fax (514) 864-9774.

Anyone having comments to make on this matter is asked to send them in writing, before the expiry of the 45-day period, to the undersigned at 1200, route de l'Église, 9e étage, Sainte-Foy (Québec) G1V 4M1.

LINDA GOUPIL,
Minister of Justice

Regulation to amend the Regulation respecting the register of personal and movable real rights

Civil Code of Québec
(1991, c. 64, ss. 2984, 3012 and 3024)

An Act respecting the implementation of the reform of the Civil Code
(1992, c. 57, s. 165)

An Act respecting registry offices
(R.S.Q., c. B-9, s. 5)

1. The Regulation respecting the register of personal and movable real rights[1] is amended by substituting, in the chapter headings in the French version, the words "CHAPITRE I" for "CHAPITRE PREMIER", and, in the chapter headings in the English version, the words "CHAPTER III" for "CHAPTER II", "CHAPTER IV" for "CHAPTER III", "CHAPTER V" for "CHAPTER IV", "CHAPTER VI" for "CHAPTER V", and "CHAPTER VIII" for "CHAPTER VII".

2. The Regulation is amended by inserting the following after section 15:

[1] The Regulation respecting the register of personal and movable real rights, made by Order in Council 1594-93 dated 17 November 1993 (1993, *G.O.* 2, 6215), was last amended by the Regulation made by Order in Council 444-98 dated 1 April 1998 (1998, *G.O.* 2, 1513).

"**CHAPTER II**
MEASURES TO GUARANTEE THE RELIABILITY OF DOCUMENTS TRANSMITTED ELECTRONICALLY

DIVISION I
TECHNOLOGICAL STRUCTURE

15.1 Where an application for registration and the accompanying request for service are transmitted electronically, the reliability and security standards prescribed in this Chapter shall apply.

The computer system that is installed and the standards with which it must comply, in particular with respect to security, shall protect the confidentiality of the documents during transmission, ensure their nonrepudiation by establishing the identity of the applicant or of the person who sends the documents over an open communications network, and guarantee their integrity and completeness at all times.

15.2 An asymmetric cryptographic system, combined with an auxiliary symmetric cryptographic system, shall be used to ensure the reliability of the data constituting the electronic documents transmitted to the registry office.

15.3 The technological structure used for the electronic transmission of documents to the registry office shall be established in accordance with international or internationally recognized recommendations and standards, and more specifically, at a minimum, with the following criteria or criteria that are at least equivalent:

(1) International Telecommunication Union (ITU) Recommendation X.500 (11/93), in general, adopted as an international standard by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the general designation of ISO/IEC 9594:1995, for the management of the directory containing the information relating to the certificates and public keys that form an integral part of key pairs;

(2) ITU Recommendation X.509 (11/93), in particular, adopted as an international standard by ISO and IEC under the designation ISO/IEC 9594-8:1995 Information Technology — Open systems interconnection (OSI) — The Directory: Authentication framework, for the issue and storage of key pairs and signature verification and encryption certificates;

(3) American National Standards Institute (ANSI) Standard X12 for data format and markup;

(4) The American federal government's National Institute of Standards and Technology (NIST) Standard FIPS 140-1 for the DES, DSA and SHA-1 algorithms used in cryptography; and

(5) ISO/IEC 8859-1: 1988 graphic character sets (Latin alphabet No. 1) for the processing and storage of documents and their printing or conversion into hard copy.

Subsections 3 and 4 above refer to standards as they existed on 1 December 1997.

15.4 The asymmetric cryptographic system shall provide for the issue of a signing key pair by means of which the transmitted documents are signed and their source identified.

The system shall also provide for the issue of an encryption key pair to protect the confidentiality of the documents being transmitted. Confidentiality is ensured by encrypting the data by means of a randomly variable secret key generated by the symmetric cryptographic system. That key is itself encrypted with the public key that forms part of the encryption key pair of the intended recipient, namely, the registry office, which decrypts the transmitted data with its private key.

The system shall also include a hash function by means of which the registry office can verify the integrity and completeness of the documents it receives.

15.5 Each signing and encryption key pair shall consist of a unique and indissociable pair of keys, one public and the other private, that are linked mathematically. Each public key shall be referred to in a certificate which serves to bind the key to the key pair holder.

The identity of the holder is verified by means of his public key and his signature verification certificate.

15.6 The signature verification certificate and encryption certificate shall be in electronic form and shall include the following information:

(1) the distinguishing name of the key pair and certificate holder which consists of his name combined with a unique code;

(2) the signature verification public key or the encryption public key, as the case may be, together with the certificate serial number, version, issue date and expiry date; and

(3) the name of the issuer, the characteristics of the algorithm and the resulting hash code used in delivering the certificate.

15.7 The encryption certificates shall be entered in an electronic directory and kept up-to-date by the registrar of the registry office.

The directory shall include the serial numbers of the signature verification certificates and encryption certificates that have been suspended, revoked, withdrawn or deleted. The form generation software automatically verifies the validity of a certificate when documents are transmitted.

DIVISION II
ISSUE AND RENEWAL OF KEY PAIRS AND CERTIFICATES

15.8 The registrar is charged with the issue and storage of key pairs and certificates attesting to the identity of the key pair holders.

15.9 In order to send an application for registration to the registry office electronically, a person shall first obtain the appropriate key pairs and certificates. They will be issued after a notary accredited by the registrar has verified the person's identity. The person requiring that verification shall bear its cost.

15.10 The person whose identity is to be verified shall appear in person and provide accurate information and relevant supporting documents.

15.11 The notary verifying an identity shall make a note of the information required by the registrar, including the verification code selected by the applicant that only he can use to identify himself to the registrar.

The notary shall certify that the identity of the person has been established, that the identity has been verified for the purpose of obtaining key pairs and certificates for the electronic transmission of documents to the registry office and, where applicable, that the person whose identity has been established intends to send applications on his own behalf or that he is authorized to send applications on behalf of another person who is named.

He shall convey the noted information and the certified facts to the registrar electronically in a transmission signed and encrypted by means of key pairs that provide at least the same degree of security and reliability as those issued by the registrar.

15.12 Where a person who applies for key pairs and certificates has been a holder of key pairs and certificates in the preceding year, his identity verification code may be used to verify his identity providing he intends to send applications only on his own behalf.

15.13 The registrar shall send to the person whose identity has been verified, in separate deliveries, two parts of a token with which the person shall generate his signing key pair from his workstation or chip card.

The person shall also choose a password to be used primarily to initiate the process of signing, encrypting and transmitting electronic data.

The public key required to verify the holder's signature shall be sent to the registrar. The transmission is done electronically and is automatic.

15.14 After receipt of the public key forming part of the signing key pair, an encryption key pair, together with a signature verification certificate and an encryption certificate, shall be issued to the holder. Where the holder is authorized to transmit applications on behalf of another person, that information shall be linked electronically, or cross-referenced, to his signature verification certificate.

The holder shall, before transmitting documents electronically, notify the registrar of the receipt of his key pairs and certificates in order that the registrar may activate them.

15.15 A valid certificate may be renewed before its expiry date for the same term as that for which it was issued. The renewal shall be effected by means of a link-up between the holder's and the registrar's computer systems within the following time limits:

(1) within two months of the certificate's expiry date, where it was issued for one year;
(2) within four months of the certificate's expiry date, where it was issued for two years;
(3) within seven months of the certificate's expiry date, where it was issued for three years;
(4) within nine months of the certificate's expiry date, where it was issued for four years; or
(5) within twelve months of the certificate's expiry date, where it was issued for five years.

A renewal requires the generation of a new signing key pair. The new public key that is part of the key pair is sent automatically to the registrar who shall then issue to the holder the certificate relating to the signing key pair as well as the encryption key pair and certificate.

DIVISION III
OBLIGATIONS OF KEY PAIR AND CERTIFICATE HOLDERS

15.16 The holder shall use his key pairs and certificates solely for the electronic transmission of documents to the registry office.

15.17 The holder shall guarantee the security and confidentiality of the private key of each of his key pairs and of his identity verification code.

He shall notify the registrar as quickly as possible where the security or the confidentiality of a private key has been compromised, particularly where there is a danger of unauthorized access to the key or of voluntary or accidental disclosure of the password that initiates the process of electronic signing, encryption and transmission of documents, or where he believes that he has lost a private key or has had it stolen.

15.18 The holder shall destroy his key pairs where, for whatever reason, he no longer uses them or may no longer use them because of the non-renewal of a certificate, or because of its withdrawal, its deletion or its revocation or because he is no longer authorized to transmit documents on others' behalf to the registry office.

SECTION IV
VALIDITY OF KEY PAIRS AND CERTIFICATES

15.19 In the event of the loss of a password accessing a certificate related to an encryption key pair, or in the event of a breakdown, dysfunction or loss of the medium storing the certificate, the holder may request the registrar to retrieve the encryption certificate and reactivate it.

A new signing key pair shall be generated from a new token sent to the holder. The new public key that is part of the signing key pair shall be automatically transmitted to the registrar who shall then issue a new signature verification certificate to the holder and send him the key pair and encryption certificate that were recovered.

Before transmitting documents electronically, the holder shall notify the registrar of the receipt of his key pairs and certificates in order that the registrar may activate them.

15.20 Where a holder no longer wishes to use his certificates, he shall notify the registrar of the date on which he intends to cease using them and request their withdrawal. The certificates shall be withdrawn following verification of the holder's identity.

The withdrawal shall become effective when the certificate serial numbers are entered on the list of withdrawn or revoked certificates, which shall be at the latest on the first working day following the date indicated by the holder in his request or on the first working day following the verification of his identity.

15.21 Where the holder has never used his certificates, he may ask the registrar to delete them from the directory. The certificates shall be deleted at the latest on the first working day following the verification of the holder's identity.

15.22 The registrar may on his own initiative suspend or revoke key pairs and related certificates where

(1) more than six months have elapsed since the holder last used the certificates;
(2) there is reason to believe that a certificate has been altered;
(3) there is reason to believe that the security of the key pairs or certificates has been compromised;
(4) the holder is no longer authorized to transmit documents electronically on others' behalf to the registry office, provided that the registrar has been notified; or
(5) the holder fails to fulfil his obligations.

The registrar shall suspend the key pairs and certificates before revoking them and, except in the situation described in subparagraph 4 of the first paragraph, notify the holder, by any manner providing proof of delivery, that his certificate has been suspended and that he intends to revoke it. Any comments by the holder shall be submitted within 15 days from the date the notice was given.

Following the suspension, the certificates shall be either reactivated or revoked. The revocation shall take effect when the certificate serial numbers are entered on the list of withdrawn or revoked certificates, which shall be at the latest one working day following the revocation.

15.23 Where a holder is no longer authorized to transmit documents electronically to the registry office on behalf of another person, that person shall notify the registrar accordingly.

15.24 The registrar shall refuse to issue, for a period of two years from the revocation, new key pairs and certificates for the transmission of documents to the registry office to a person whose key pairs and certificates were revoked as a result of a failure to fulfil his obligations.

15.25 Where the holder of key pairs and certificates requests the retrieval or withdrawal of a certificate, the deletion of a certificate from a directory, or the correction of the unique code that forms part of his distinguishing name, his identity may be verified by means of his identity verification code.

15.26 The holder shall be notified of any correction, renewal or withdrawal of a certificate, reactivation of a certificate following its suspension or revocation, or deletion of a certificate from a directory. He shall also be notified of any refusal to issue a certificate and the grounds therefor.".

3. The following is substituted for Divisions II and III of CHAPTER II:

"**DIVISION II**
MEDIUM AND TRANSMISSION

22. An application for registration may be in paper form. It may also be submitted in electronic form insofar as it is generated by means of the form generation software provided to the applicant by the registry office.

It may be transmitted to the registry office's electronic depository in accordance with the provisions of CHAPTER II relating to the electronic transmission of documents where it is generated and delivered by means of that software.

23. The application for registration in the form of a notice shall be prepared by using either the paper form provided by the registry office or the software referred to in section 22. The form to be completed shall be as prescribed in the Schedules to this Regulation and shall be appropriate to the type of application filed.

23.1 The form generation software shall be locked in by means of a hash code that will guarantee its integrity. The applicant shall not modify the software and he shall use one of the versions in use at the registry office.

23.2 An application form consists of texts and key words in addition to headings and spaces that shall be filled in according to the instructions relating to the type of application filed. The basic information making up the form may be arranged differently depending on whether the paper form or electronic form is used.

23.3 An application for registration in paper form shall be submitted on paper measuring 215 x 355 mm and weighing at least 75g/m^2 per ream; an application in the form of a notice shall be printed on only one side of the sheet.

23.4 An application for registration in paper form may not be a copy; it shall be typed, printed or written in block letters using good quality ink. The characters shall be clear, neat and legible, without deletions or alterations.

It shall bear the applicant's handwritten signature and his name shall be typed, printed or written in block letters under the signature or in the space provided on the application form.

It may be filed in person at the registry office or sent by mail.

23.5 An application for registration in electronic form shall consist of the data constituting the application form and inserted information that appear as screen pages. The form and inserted information data are linked electronically or by reference.

23.6 An application for registration in electronic form shall be signed by means of the digital signature process by the holder of the key pair used to transmit data electronically to the registry office. Only one signature is required for the transmission of a set of documents consisting of several applications for registration and one request for service.

The holder shall make the transmission by file transfer to the registry office's electronic depository where it will be received by the registrar. The holder shall attach his signature verification certificate to the transmitted data.

23.7 The data shall be considered received only where they have been transmitted in full and where the registrar is able to access and decrypt them.

23.8 Upon receipt of an application for registration in electronic form, the registrar shall make sure that the key pair holder's signature verification certificate and digital signature are valid and that the transmitted data are intact.".

4. The Regulation is amended by substituting the following for the heading of DIVISION IV of CHAPTER II:

"**DIVISION III**
CONTENT OF APPLICATIONS".

5. The Regulation is amended by inserting the following after section 47:

"**47.1** Where the registrar must provide a copy of a digitally signed electronic document, the document shall be converted into hard copy from the data that was received and decrypted and whose integrity has been verified. The information constituting the form shall be added to these data.

The name of the signatory resulting from the verification of his identify and, if applicable, the name of the

person on whose behalf the application for registration was transmitted shall appear on the hard copy.".

6. The following is substituted for CHAPTER VI of the Regulation:

"**CHAPTER VII**
CONSERVATION, REPRODUCTION AND TRANSFER

49. An application for registration and any supporting document may, where they are in paper form, be reproduced on microfilm or on a non-rewritable optical medium.

A backup copy of the microfilm or optical disks shall be stored elsewhere than at the registry office.

49.1 The data constituting the applications for registration and documents transmitted in electronic form to the registry office shall be conserved as received.

They may however be transferred to a non-rewritable optical medium in order to protect the data received, in particular against accidental alterations.

50. Cancelled entries or entries cancelling other entries may be transferred to a magnetic or non-rewritable optical medium.".

7. This Regulation comes into force on the fifteenth day following the date of its publication in the *Gazette officielle du Québec*.

2768

Draft Regulation

An Act respecting the conservation and development of wildlife
(R.S.Q., c. C-61.1)

Salmon fishing controlled zones

Notice is hereby given, in accordance with sections 10 and 11 of the Regulations Act (R.S.Q., c. R-18.1), that the Regulation respecting salmon fishing controlled zones, the text of which appears below, may be made by the Government upon the expiry of 45 days following the date of this publication.

The purpose of the draft Regulation is to give more latitude to ZEC managing agencies, in particular for the setting of fees and for certain management procedures.

To that end, the Regulation proposes:

— a regulation specific to salmon fishing ZECs;
— more flexibility in the setting of fees;
— the assignment of 20 % of limited places according to procedures decided in a general meeting, as is the case now, but with more flexibility;
— the possibility that 2 % of the days of access be assigned for promotional purposes;
— the replacement of the prohibition against automobile races and rallies by a delegation of the power to decide to the managing agencies;
— the showing of licences upon registration.

To date, study of the matter has shown no negative impact on businesses, particularly on small and medium-sized businesses. On the contrary, the changes should allow for a better financing of ZEC managing agencies through greater flexibility in the setting of fees, while favouring the various customers concerned. They also facilitate the marketing of available places in the low season.

Further information may be obtained by contacting:

Mr. Gaétan Hamel
Faune et Parcs
Service de la réglementation
675, boulevard René-Lévesque Est, 10e étage, boîte 91
Québec (Québec)
G1R 5V7

Tel: (418) 521-3880, ext. 4094
Fax: (418) 528-0834
E-mail: gaetan.hamel@mef.gouv.qc.ca

Any interested person having comments to make on the matter is asked to send them in writing, before the expiry of the 45-day period, to the Minister responsible for Wildlife and Parks, 700, boulevard René-Lévesque Est, 29e étage, Québec (Québec) G1R 5H1.

GUY CHEVRETTE,
Minister responsible for Wildlife and Parks