

## Draft Regulation

Notaries Act  
(chapter N-3)

### Notaries

#### — Digital official signature

Notice is hereby given, in accordance with sections 10 and 11 of the Regulations Act (chapter R-18.1), that the Regulation respecting a notary's digital official signature, made by the board of directors of the Chambre des notaires du Québec and appearing below, may be submitted to the Government for approval, with or without amendment, on the expiry of 45 days following this publication.

The draft Regulation prescribes the conditions and procedure for authorizing the use, by a notary, of an official signature affixed by means of a technological process and those for revoking such authorization, and determining the technological process that must be used to affix it and the minimal conditions a certification service provider must meet.

The draft Regulation has no impact on the public or on enterprises, including small and medium-sized businesses.

Further information may be obtained by contacting Nathalie Provost, notary, Affaires juridiques, Services juridiques et relations institutionnelles, Chambre des notaires du Québec, 101-2045, rue Stanley, Montréal (Québec) H3A 2V4; telephone: 1 800 263-1793 or 514 879-1793, extension 5921; email: servicesjuridiques@cnq.org.

Any person wishing to comment on the draft Regulation is requested to submit written comments within the 45-day period to Diane Legault, Chair of the Office des professions du Québec, 800, place D'Youville, 10<sup>e</sup> étage, Québec (Québec) G1R 5Z3. The comments will be forwarded by the Office to the Minister of Justice and may also be sent to the professional order that made the Regulation and to interested persons, departments and bodies.

DIANE LEGAULT,  
*Chair of the Office des  
professions du Québec*

## Regulation respecting a notary's digital official signature

Notaries Act  
(chapter N-3, s. 98, 1st par., subpar. (1))

### DIVISION I PURPOSE

**1.** The purpose of this regulation is to determine, in addition to the provisions under the Act to Establish a Legal Framework for Information Technology (chap-

ter C-1.1), the technological process to be used by a notary to affix his official signature using such means, the conditions and procedure for authorizing the use of an official signature affixed by means of such a technological process, those for revoking such an authorization, and the minimal conditions a certification service provider must meet.

### DIVISION II TECHNOLOGICAL PROCESS

**2.** The technological process by means of which a notary may affix his official signature is an asymmetric cryptographic system supported by a public-key infrastructure. It is his digital official signature.

### DIVISION III AUTHORIZATION TO USE AND REVOCATION

#### §1. *Authorization to use*

**3.** The secretary of the Order authorizes the notary who makes an application to that effect, using the document established by the Order, to use a digital official signature.

To obtain this authorization, the notary must have his identity verified by another notary and must attach, to his application, the attestation of this verification using the document established by the Order.

In his application, the notary must undertake:

- (1) to use his digital official signature only in the practice of his profession;
- (2) not to allow the use thereof by a third person;
- (3) to ensure the security and the confidentiality of every password or secret element related to his digital official signature.

Furthermore, if he becomes aware that the security or the confidentiality of any password or secret element related to his digital official signature has been compromised or if he has reasonable grounds to believe so, he undertakes to immediately notify thereof:

- (1) the secretary of the Order;
- (2) the certification service provider;
- (3) any person who may have received a document bearing his digital official signature while, in fact, it was affixed by a third person.

The notary must pay the fees relating to his application for an authorization.

## §2. Revocation of the authorization

**4.** The secretary of the Order must revoke the authorization given to the notary in each of the following cases:

- (1) on the written application of the notary;
- (2) the notary has been removed from the roll of the Order;
- (3) the notary fails to fulfil one of the undertakings provided under section 3;
- (4) any other situation where he is informed that the confidentiality or the security of the password or of the secret elements related to the digital official signature has been compromised;
- (5) on the written application of the certification service provider, when the notary fails to pay the fees relating to the use of his digital official signature.

The secretary of the Order must inform the notary and the certification service provider of the revocation.

## DIVISION IV CERTIFICATION SERVICE PROVIDER

**5.** Only a certification service provider that has been authorized by the Order and has entered into an agreement with the Order may issue a digital official signature to a notary.

**6.** The Order authorizes a certification service provider that makes an application to that effect and that meets the following minimal conditions:

- (1) it has a certification policy that complies with RFC 3647 and RFC 3280 documents developed by the Internet Engineering Task Force and that includes a procedure for identity verification;
- (2) it issues keys and certificates by means of a public-key infrastructure;
- (3) it has a certificate directory that meets the International Telecommunication Union (ITU) Recommendation X.500;
- (4) it issues certificates that comply with the ITU Recommendation X.509;
- (5) it issues keys that consist of a unique and indissociable pair of keys, one public and the other private, which allow the signing of technology-based documents and the identification of the signer;

(6) it issues certificates that include at least the following elements:

- a) the distinguishing name of the notary combined with a unique code;
- b) a mention to the effect that he is a notary;

(7) it enters the signature certificates into a directory held on a media based on information technology and keeps it up-to-date. This directory must include, notably, the serial numbers of the signature certificates that are valid, suspended, cancelled, or archived.

References to a standard provided under subparagraphs 1°, 3°, and 5° of the first paragraph refer to the most recent edition published by the body and include all subsequent amendments made thereto.

**7.** The certification service provider must make sure that the notary has the authorization of the secretary of the Order before it issues his digital official signature to him.

**8.** When the certification service provider is informed or determines that the security or the confidentiality of the password or secret elements related to a notary's digital official signature may be compromised, it must notify the secretary of the Order and the notary to that effect.

The certification service provider must make sure that the secretary of the Order has revoked a notary's authorization before it revokes his digital official signature.

## DIVISION V TRANSITIONAL AND FINAL PROVISIONS

**9.** The personal code or mark assigned to a notary by the secretary of the Order before (*enter the date of the coming into force of this regulation*) is his digital official signature and the notary may use it, subject to a written undertaking on his part in compliance with the one provided under section 3, if the certification service provider that issued it meets the conditions provided under sections 5 and 6.

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

103788