



CANADA

CONSOLIDATION

CODIFICATION

# Secure Electronic Signature Regulations

# Règlement sur les signatures électroniques sécurisées

SOR/2005-30

DORS/2005-30

Current to May 2, 2012

À jour au 2 mai 2012

Last amended on March 10, 2011

Dernière modification le 10 mars 2011

Published by the Minister of Justice at the following address:  
<http://laws-lois.justice.gc.ca>

Publié par le ministre de la Justice à l'adresse suivante :  
<http://lois-laws.justice.gc.ca>

OFFICIAL STATUS  
OF CONSOLIDATIONS

CARACTÈRE OFFICIEL  
DES CODIFICATIONS

Subsections 31(1) and (3) of the *Legislation Revision and Consolidation Act*, in force on June 1, 2009, provide as follows:

Les paragraphes 31(1) et (3) de la *Loi sur la révision et la codification des textes législatifs*, en vigueur le 1<sup>er</sup> juin 2009, prévoient ce qui suit:

Published  
consolidation is  
evidence

**31.** (1) Every copy of a consolidated statute or consolidated regulation published by the Minister under this Act in either print or electronic form is evidence of that statute or regulation and of its contents and every copy purporting to be published by the Minister is deemed to be so published, unless the contrary is shown.

**31.** (1) Tout exemplaire d'une loi codifiée ou d'un règlement codifié, publié par le ministre en vertu de la présente loi sur support papier ou sur support électronique, fait foi de cette loi ou de ce règlement et de son contenu. Tout exemplaire donné comme publié par le ministre est réputé avoir été ainsi publié, sauf preuve contraire.

Codifications  
comme élément  
de preuve

...

[...]

Inconsistencies  
in regulations

(3) In the event of an inconsistency between a consolidated regulation published by the Minister under this Act and the original regulation or a subsequent amendment as registered by the Clerk of the Privy Council under the *Statutory Instruments Act*, the original regulation or amendment prevails to the extent of the inconsistency.

(3) Les dispositions du règlement d'origine avec ses modifications subséquentes enregistrées par le greffier du Conseil privé en vertu de la *Loi sur les textes réglementaires* l'emportent sur les dispositions incompatibles du règlement codifié publié par le ministre en vertu de la présente loi.

Incompatibilité  
— règlements

NOTE

This consolidation is current to May 2, 2012. The last amendments came into force on March 10, 2011. Any amendments that were not in force as of May 2, 2012 are set out at the end of this document under the heading "Amendments Not in Force".

NOTE

Cette codification est à jour au 2 mai 2012. Les dernières modifications sont entrées en vigueur le 10 mars 2011. Toutes modifications qui n'étaient pas en vigueur au 2 mai 2012 sont énoncées à la fin de ce document sous le titre « Modifications non en vigueur ».

TABLE OF PROVISIONS

TABLE ANALYTIQUE

Section		Page	Article		Page
	Secure Electronic Signature Regulations			Règlement sur les signatures électroniques sécurisées	
1	INTERPRETATION	1	1	DÉFINITIONS	1
2	TECHNOLOGY OR PROCESS	2	2	TECHNOLOGIE OU PROCÉDÉ	2
5	PRESUMPTION	4	5	PRÉSUMPTION	4
6	COMING INTO FORCE	4	6	ENTRÉE EN VIGUEUR	4

Registration  
SOR/2005-30 February 1, 2005

PERSONAL INFORMATION PROTECTION AND  
ELECTRONIC DOCUMENTS ACT  
CANADA EVIDENCE ACT

**Secure Electronic Signature Regulations**

P.C. 2005-57 February 1, 2005

Whereas the Governor in Council is satisfied that the technology or process prescribed in the annexed *Secure Electronic Signature Regulations* can be proved to meet the requirements set out in paragraphs 48(2)(a) to (d) of the *Personal Information Protection and Electronic Documents Act*<sup>a</sup>;

Therefore, Her Excellency the Governor General in Council, on the recommendation of the Treasury Board, pursuant to subsection 48(1) of the *Personal Information Protection and Electronic Documents Act*<sup>a</sup> and paragraph 31.4(a)<sup>b</sup> of the *Canada Evidence Act*, hereby makes the annexed *Secure Electronic Signature Regulations*.

Enregistrement  
DORS/2005-30 Le 1<sup>er</sup> février 2005

LOI SUR LA PROTECTION DES RENSEIGNEMENTS  
PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES  
LOI SUR LA PREUVE AU CANADA

**Règlement sur les signatures électroniques sécurisées**

C.P. 2005-57 Le 1<sup>er</sup> février 2005

Attendu que la gouverneure en conseil est convaincue qu'il peut être établi que la technologie ou le procédé prévu dans le projet de règlement intitulé *Règlement sur les signatures électroniques sécurisées*, ci-après, est conforme aux exigences des alinéas 48(2)a) à d) de la *Loi sur la protection des renseignements personnels et les documents électroniques*<sup>a</sup>,

À ces causes, sur recommandation du Conseil du Trésor et en vertu du paragraphe 48(1) de la *Loi sur la protection des renseignements personnels et les documents électroniques*<sup>a</sup> et de l'alinéa 31.4a)<sup>b</sup> de la *Loi sur la preuve au Canada*, Son Excellence la Gouverneure générale en conseil prend le *Règlement sur les signatures électroniques sécurisées*, ci-après.

---

<sup>a</sup> S.C. 2000, c. 5

<sup>b</sup> S.C. 2000, c. 5, s. 56

---

<sup>a</sup> L.C. 2000, ch. 5

<sup>b</sup> L.C. 2000, ch. 5, art. 56

INTERPRETATION

1. The following definitions apply in these Regulations.

“Act” means the *Personal Information Protection and Electronic Documents Act*. (*Loi*)

“asymmetric cryptography” means a cryptographic system that relies on key pairs. (*système de chiffrement à clé publique*)

“certification authority” means a person or entity that issues digital signature certificates and that is listed as such on the website of the Treasury Board Secretariat. (*autorité de certification*)

“digital signature certificate”, in respect of a person, means an electronic document that

- (a) identifies the certification authority that issued it and is digitally signed by that certification authority;
- (b) identifies, or can be used to identify, the person; and
- (c) contains the person's public key. (*certificat de signature numérique*)

“entity” includes any federal department, branch, office, board, agency, commission, corporation or body for the administration of the affairs of which a minister of the Crown is accountable to Parliament. (*entité*)

“hash function” means an electronic one-way mathematical process that converts data contained in an electronic document into a message digest that is unique to that data in a way that, were that data changed, it would, on conversion, result in a changed message digest. (*fonction de hachage*)

“key pair” means a pair of keys held by or for a person that includes a private key and a public key that are mathematically related to, but different from, each other. (*biclé*)

“private key” means a string of data that

- (a) is used in asymmetric cryptography to encrypt data contained in an electronic document; and

DÉFINITIONS

1. Les définitions qui suivent s'appliquent au présent règlement.

«autorité de certification» Personne ou entité qui délivre des certificats de signature numérique et qui est inscrite en cette qualité sur le site Web du Secrétariat du Conseil du Trésor. (*certification authority*)

«biclé» Paire de clés détenue par ou pour une personne et comportant une clé privée et une clé publique qui sont mathématiquement liées tout en étant différentes l'une de l'autre. (*key pair*)

«certificat de signature numérique» À l'égard d'une personne, document électronique qui, à la fois :

- a) identifie l'autorité de certification qui l'a délivré et est signé numériquement par celle-ci;
- b) identifie la personne ou peut servir à l'identifier;
- c) renferme la clé publique de cette personne. (*digital signature certificate*)

«clé privée» Suite de données qui, à la fois :

- a) est utilisée dans un système de chiffrement à clé publique pour chiffrer des données contenues dans un document électronique;
- b) est propre à la personne qui est identifiée dans le certificat de signature numérique ou au moyen de celui-ci, et correspond exclusivement à la clé publique d'une biclé. (*private key*)

«clé publique» Suite de données contenue dans un certificat de signature numérique qui, à la fois :

- a) est utilisée dans un système de chiffrement à clé publique pour déchiffrer des données contenues dans un document électronique qui ont été chiffrées au moyen de la clé privée d'une biclé;
- b) correspond exclusivement à cette clé privée. (*public key*)

«entité» Sont assimilés à une entité un ministère, une direction, un bureau, un conseil, une commission, un ser-

(b) is unique to the person who is identified in, or can be identified through, a digital signature certificate and corresponds only to the public key in that certificate. (*clé privée*)

“public key” means a string of data contained in a digital signature certificate that

(a) is used in asymmetric cryptography to decrypt data contained in an electronic document that was encrypted through the application of the private key in the key pair; and

(b) corresponds only to the private key in the key pair. (*clé publique*)

SOR/2011-71, s. 1(E).

#### TECHNOLOGY OR PROCESS

2. For the purposes of the definition “secure electronic signature” in subsection 31(1) of the Act, a secure electronic signature in respect of data contained in an electronic document is a digital signature that results from completion of the following consecutive operations:

(a) application of the hash function to the data to generate a message digest;

(b) application of a private key to encrypt the message digest;

(c) incorporation in, attachment to, or association with the electronic document of the encrypted message digest;

(d) transmission of the electronic document and encrypted message digest together with either

(i) a digital signature certificate, or

(ii) a means of access to a digital signature certificate; and

(e) after receipt of the electronic document, the encrypted message digest and the digital signature certificate or the means of access to the digital signature certificate,

vice, un office, une personne morale ou autre organisme dont un ministre est responsable devant le Parlement. (*entity*)

«fonction de hachage» Opération mathématique unidirectionnelle électronique qui convertit des données contenues dans un document électronique en un condensé propre à ces données de sorte que, advenant toute modification de celles-ci, un condensé différent en résulterait. (*hash function*)

«Loi» La *Loi sur la protection des renseignements personnels et les documents électroniques*. (*Act*)

«système de chiffrement à clé publique» Système de chiffrement faisant appel aux biclés. (*asymmetric cryptography*)

DORS/2011-71, art. 1(A).

#### TECHNOLOGIE OU PROCÉDÉ

2. Pour l'application de la définition de «signature électronique sécurisée», au paragraphe 31(1) de la Loi, la signature électronique sécurisée à l'égard des données contenues dans un document électronique est la signature numérique qui résulte de l'exécution des opérations consécutives suivantes :

a) l'application de la fonction de hachage aux données pour générer un condensé;

b) l'application d'une clé privée au condensé pour le chiffrer;

c) l'incorporation, l'adjonction ou l'association du condensé ainsi chiffré au document électronique;

d) la transmission du document électronique et du condensé chiffré accompagnés :

(i) soit du certificat de signature numérique,

(ii) soit d'un moyen permettant d'accéder à ce certificat;

e) à la réception du document électronique et du condensé chiffré et, selon le cas, du certificat de signature numérique ou du moyen permettant d'accéder à celui-ci :

- (i) application of the public key contained in the digital signature certificate to decrypt the encrypted message digest and produce the message digest referred to in paragraph (a),
- (ii) application of the hash function to the data contained in the electronic document to generate a new message digest,
- (iii) verification that, on comparison, the message digests referred to in paragraph (a) and subparagraph (ii) are identical, and
- (iv) verification that the digital signature certificate is valid in accordance with section 3.

3. (1) A digital signature certificate is valid if, at the time when the data contained in an electronic document is digitally signed in accordance with section 2, the certificate

- (a) is readable or perceivable by any person or entity who is entitled to have access to the digital signature certificate; and
- (b) has not expired or been revoked.

(2) In addition to the requirements for validity set out in subsection (1), when the digital signature certificate is supported by other digital signature certificates, in order for the digital signature certificate to be valid, the supporting certificates must also be valid in accordance with that subsection.

4. (1) Before recognizing a person or entity as a certification authority, the President of the Treasury Board must verify that the person or entity has the capacity to issue digital signature certificates in a secure and reliable manner within the context of these Regulations and paragraphs 48(2)(a) to (d) of the Act.

(2) Every person or entity that is recognized as a certification authority by the President of the Treasury Board shall be listed on the website of the Treasury Board Secretariat.

- (i) l'application de la clé publique contenue dans le certificat de signature numérique pour déchiffrer le condensé et produire le condensé visé à l'alinéa a),
- (ii) l'application de la fonction de hachage aux données contenues dans le document électronique pour générer un nouveau condensé,
- (iii) la comparaison entre le condensé visé à l'alinéa a) et celui visé au sous-alinéa (ii) pour établir qu'ils sont identiques,
- (iv) la vérification de la validité du certificat de signature numérique en conformité avec l'article 3.

3. (1) Le certificat de signature numérique est valide si, au moment où les données contenues dans un document électronique sont numériquement signées conformément à l'article 2, les conditions suivantes sont réunies :

- a) le certificat est lisible ou perceptible par la personne ou l'entité autorisée à y avoir accès;
- b) il n'est ni expiré ni révoqué.

(2) En plus des exigences prévues au paragraphe (1), le certificat de signature numérique qui est fondé sur d'autres certificats de signature numérique est valide si ceux-ci sont également valides aux termes de ce paragraphe.

4. (1) Avant de reconnaître à une personne ou entité la qualité d'autorité de certification, le président du Conseil du Trésor doit vérifier si elle est en mesure de délivrer les certificats de signature numérique de manière fiable et sécuritaire aux termes du présent règlement et des alinéas 48(2)a) à d) de la Loi.

(2) Toute personne ou entité dont la qualité d'autorité de certification est reconnue par le président du Conseil du Trésor est inscrite sur le site Web du Secrétariat du Conseil du Trésor.

**PRESUMPTION**

**5.** When the technology or process set out in section 2 is used in respect of data contained in an electronic document, that data is presumed, in the absence of evidence to the contrary, to have been signed by the person who is identified in, or can be identified through, the digital signature certificate.

**COMING INTO FORCE**

**6.** These Regulations come into force on the day on which they are registered.

**PRÉSUMPTION**

**5.** Si la technologie ou le procédé visé à l'article 2 est utilisé à l'égard des données contenues dans un document électronique, ces données sont présumées, en l'absence de preuve contraire, avoir été signées par la personne identifiée dans le certificat de signature numérique ou au moyen de celui-ci.

**ENTRÉE EN VIGUEUR**

**6.** Le présent règlement entre en vigueur à la date de son enregistrement.