

La signature et la certification

Loi concernant le cadre juridique des technologies de l'information
art. 40 à 43 et 46,
47 à 62, 75, 77



Moyens de lier une personne et une chose

Procédés ou moyens permettant de :	Exemples
1) • confirmer l'identité d'une personne ou • confirmer l'identification d'une association, d'une société, d'un État ou sa localisation	➤ Un document (art. 40), un document technologique, tel un certificat (art. 47), les mesures biométriques (selon les balises de l'article 44)
et • confirmer leur lien avec le document	➤ La signature par tout procédé (art. 39), un certificat (art. 47)
2) • identifier le document, et au besoin sa provenance et sa destination à un moment particulier	➤ L'identifiant (art. 46), un certificat (art. 46, 47)

La signature et la certification

- Concernent les qualités des MOYENS utilisés pour établir un lien entre personnes et objets
- la loi énonce des standards... des qualités que doivent présenter les procédés utilisés

Pour favoriser l'interopérabilité

- Dans une grande variété de contextes techniques
- Les lois sont rédigées en forme de principes et énoncent des résultats à atteindre, des standards à rencontrer

Le lien entre un document et une personne, une association, une société ou l'État

- peut être assuré par tout procédé ou par une combinaison de moyens du moment qu'ils permettent d'atteindre les résultats énoncés à l'article 38:
- identifier le document, au besoin sa provenance et sa destination
- et confirmer l'identité d'une personne et son lien avec le document identifié

Les qualités que doivent posséder les mécanismes utilisés pour établir des liens

- doit s'appuyer sur la vérification
- l'obligation de respecter la loi lors de cette opération.
- la confirmation de l'identité ou de l'identification: peut se faire au moyen d'un document, entre autres un certificat, dont l'intégrité est assurée.

L'identification

- c'est l'action —le processus— d'identifier
- de reconnaître une personne, à certains traits non équivoques qui lui sont spécifiques.
- un processus d'information par lequel on compare de l'information afin d'avoir le degré de certitude requis à l'égard des qualités de la personne avec laquelle on entre en contact.

Les pièces d'identité

- Lorsque la loi exige de fournir une attestation, une carte, un certificat, une pièce ou une preuve d'identité ou un autre document servant à établir l'identité d'une personne, cette exigence peut être satisfaite au moyen d'un document faisant appel à la technologie appropriée à son support. (art. 42)

Quiconque fait valoir, pour preuve de son identité ou de celle d'une autre personne, un document technologique

- qui présente une caractéristique personnelle, une connaissance particulière ou qui indique que la personne devant être identifiée possède un objet qui lui est propre,
- est tenu de préserver l'intégrité du document qu'il présente.

Un document d'identité doit être protégé

- contre l'interception lorsque sa conservation ou sa transmission sur un réseau de communication rend possible l'usurpation de l'identité de la personne visée par ce document.
- sa confidentialité doit être protégée, le cas échéant, et sa consultation doit être journalisée.

Les identifiants d'objets ou de documents

- Lorsqu'un document utilisé pour effectuer une communication en réseau doit être conservé pour constituer une preuve, son identifiant doit être conservé avec lui pendant tout le cycle de vie du document par la personne qui est responsable du document.
- L'identifiant se compose d'un nom de référence distinct et non ambigu dans l'ensemble des dénominations locales où il est inscrit, ainsi que des extensions nécessaires pour joindre ce nom à des ensembles de dénominations universels.

L'accessibilité de l'identifiant

- L'identifiant du document doit être accessible au moyen d'un service de répertoire, dont une des fonctions est de relier un identifiant à sa localisation. Le lien entre un identifiant et un objet peut être garanti par un certificat lequel est lui-même accessible au moyen d'un service de répertoire qui peut être consulté par le public.
- Pour permettre d'établir la provenance ou la destination du document à un moment déterminé, les autres objets qui ont servi à effectuer la communication, comme les certificats, les algorithmes et les serveurs d'envoi ou de réception, doivent pouvoir être identifiés et localisés, au moyen des identifiants alors attribués à chacun de ces objets.

La signature

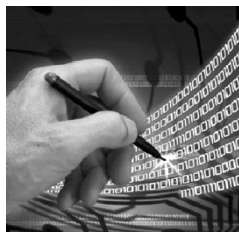
- Peut servir à l'établissement d'un lien entre le signataire et le document
 - elle peut être apposée au moyen de tout procédé qui satisfait aux exigences de l'art. 2827 CCQ
- La signature d'une personne apposée à un document technologique lui est opposable
 - lorsqu'il s'agit d'un document dont l'intégrité est assurée et qu'au moment de la signature et depuis, le lien entre la signature et le document est maintenu

définition

- 2827. La signature consiste dans l'apposition qu'une personne fait à un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement.

Éléments de la signature

- une marque
- fait à un acte
- personnelle
- utilisée de façon courante



L'apposition d'un sceau, d'un cachet, d'un tampon, d'un timbre ou d'un autre instrument

- Pour protéger l'intégrité du document ou en manifester la fonction d'original
- Pour identifier une personne
- Pour assurer la confidentialité



La certification: « assurance donnée par écrit »

La loi édicte les principes et normes relatifs à:

- l'utilisation des certificats et des répertoires
- l'encadrement des activités des personnes proposant des services de certification.
- prévoit les conditions régissant l'offre de services de certification ou de répertoire.
- aussi un mécanisme d'accréditation volontaire des prestataires de service de certification
- et précise la responsabilité incombant à ceux qui émettent, utilisent ou se fient à un certificat.

La certification et les tiers de confiance: les prestataires de services de certification

- Un moyen afin d'obtenir un niveau plus élevé de certitude
- « autorité de certification »: *“autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer leur clé publique et leur certificat”*.
 - UIT-T, Recommandation X.509, Annuaire - Cadre d'authentification, Fasc. VIII.8, 1988, art. 3.3 c).

Un certificat peut servir à établir un ou plusieurs faits dont:

- la confirmation de l'identité d'une personne,
- l'identification d'une société, d'une association ou de l'État,
- l'exactitude d'un identifiant d'un document ou d'un autre objet,
- l'existence de certains attributs d'une personne,
- un document ou d'un autre objet ou encore du lien entre eux et un dispositif d'identification ou de localisation tangible ou logique.

Le contenu minimal du certificat

- 1° le nom distinctif du prestataire de services qui délivre le certificat ainsi que sa signature;
 - 2° la référence à l'énoncé de politique du prestataire de services de certification, y compris ses pratiques, sur lequel s'appuient les garanties qu'offre le certificat qu'il délivre;
 - 3° la version de certificat et le numéro de série du certificat;
 - 4° le début et la fin de sa période de validité ;
- Autres infos si certificat d'identité ou d'attribut

Le répertoire

- doit être constitué conformément aux normes ou standards techniques approuvés par un organisme reconnu;
- doit être accessible au public, soit directement ou au moyen d'un dispositif de consultation sur place ou à distance;
- mais... il ne peut rendre public le motif pour lequel un certificat a pu être suspendu ou annulé.

Les services de certification et de répertoire

- Les services de certification
 - comprennent la vérification de l'identité de personnes et la délivrance de certificats confirmant leur identité, l'identification d'une association, d'une société ou de l'État ou l'exactitude de l'identifiant d'un objet.
- Les services de répertoire
 - comprennent l'inscription des certificats et des identifiants dans un répertoire accessible au public et la confirmation de la validité des certificats répertoriés ainsi que leur lien avec ce qu'ils confirment.

Les obligations du prestataire de services

- présenter des garanties d'impartialité par rapport à la personne ou l'objet visé par la certification, même s'il n'est pas un tiers à leur égard.
- assurer l'intégrité du certificat qu'il délivre au cours de tout son cycle de vie, y compris en cas de modification, de suspension, d'annulation ou d'archivage, ou en cas de mise à jour d'un renseignement qu'il contient.
- être en mesure de confirmer le lien entre le dispositif d'identification ou de localisation, tangible ou logique, et la personne, l'association, la société, l'État ou l'objet identifié ou localisé au moyen du dispositif.

Autres obligations des prestataires de services de certification

- Relatives à l'identification
- Aux identifiants

Accréditation des certificateurs

- ACCRÉDITATION emporte une PRÉSUMPTION DE CONFORMITÉ À LA LOI DES CERTIFICATS DÉLIVRÉS
- Qui l'accorde?
- Une personne ou organisme désigné par le gouvernement

L'accréditation...

- Comment?
- Le gouvernement peut déterminer par règlement:
 - 1- la procédure d'accréditation;
 - 2- les conditions d'octroi;
 - 3- les délais d'obtention de l'accréditation ou d'une modification de ses conditions;
 - 4- les conditions relatives au renouvellement, à la suspension ou à l'annulation de l'accréditation; et
 - 5- les frais afférents.

Selon quels critères?

- L'article 55 indique sur quels critères minimums on se base pour accorder une accréditation, et qui s'ajoutent à l'information contenue dans l'énoncé de politique.

L'inscription dans un registre

- prestataires accrédités ou dont les services sont reconnus équivalents doivent être inscrits dans un registre accessible au public.
(deuxième alinéa de l'article 54)

La fausse représentation_

- le fait de délivrer un document présenté comme un certificat servant à confirmer (entre autres) l'identité d'une personne :
 - i) alors qu'aucune vérification n'a été faite; ou que
 - ii) l'insuffisance de la vérification équivaut à une absence de vérification
- constitue une fausse représentation.

Le PSC qui a des motifs raisonnables de croire que...

- le dispositif a été volé ou perdu ou que sa confidentialité est compromise
- doit en aviser les personnes mentionnées à l'art. 58

Obligation de celui qui fournit des renseignements afin d'obtenir pour lui-même la délivrance d'un certificat

- informer le prestataire de services de certification, dans les meilleurs délais, de toute modification de ces renseignements les obligations de la personne qui veut agir en se fondant sur le certificat.

Les services de certification et de répertoire

- Les services de certification
 - comprennent la vérification de l'identité de personnes et la délivrance de certificats confirmant leur identité, l'identification d'une association, d'une société ou de l'État ou l'exactitude de l'identifiant d'un objet.
- Les services de répertoire
 - comprennent l'inscription des certificats et des identifiants dans un répertoire accessible au public et la confirmation de la validité des certificats répertoriés ainsi que leur lien avec ce qu'ils confirment.

Les obligations relatives au certificat

- **61.** Le prestataire de services de certification et de répertoire, le titulaire visé par le certificat et la personne qui agit en se fondant sur le certificat
- sont, à l'égard des obligations qui leur incombent en vertu de la présente loi, tenus à une obligation de moyens.

**Responsabilité du PSC et de
répertoire, du titulaire visé par le
certificat et de la personne qui
agit en se fondant sur le certificat**

- Responsabilité conjointe
- En principe pour leur part de faute
- Si personne n'est en faute, responsabilité à parts égales
- Impossible d'exclure sa responsabilité
