POLITIQUES DE CERTIFICATS
DE SIGNATURE ET DE CONFIDENTIALITÉ
DU REGISTRE DES DROITS PERSONNELS ET RÉELS MOBILIERS

Version 1.1
1er août 2004

Québec

Table des matières

INTRODUCTION

1. RENSEIGNEMENTS GÉNÉRAUX 8

1.1 Identification 8
1.1.1 Nom des politiques 8
1.1.2 Identifiants d'objet 8

1.2 Champ d'application des politiques 8

1.3 Coordonnées du responsable des présentes politiques 9

1.4 Entente de reconnaissance 9

1.5 Intervenants de l'ICP du RDPRM 9
1.5.1 Service de certification 9
1.5.2 AVI 10
1.5.3 Abonné 10
1.5.3.1 Abonné qui est un individu 10
1.5.3.2 Abonné qui n'est pas un individu (dispositif physique ou applicatif) 11
1.5.4 Utilisateur de certificats 11

2. PRATIQUES EN MATIÈRE D'IDENTIFICATION ET DE VÉRIFICATION DE L'IDENTITÉ 12

2.1 Vérifications relatives à la délivrance d'un certificat 12
2.1.1 Vérifications requises de l'AVI avant la délivrance d'un certificat 12
2.1.1.1 Obligation d'une rencontre physique 12
2.1.1.2 Vérification des pièces d'identité requises pour l'identification d'un demandeur 12
2.1.1.3 Vérification requises pour un abonné qui est un individu 12
2.1.1.3.1 Individu agissant pour son propre compte 12
2.1.1.3.2 Individu agissant pour le compte d'autrui 12
2.1.1.4 Vérification requises pour un abonné qui n'est pas un individu (dispositif) 13
2.1.1.5 Compte rendu de la vérification de l'identité 13
2.1.2 Vérifications requises du service de certification avant la délivrance d'un certificat 14
2.1.2.1 Lors de la demande de délivrance d'un certificat 14
2.1.2.2 Lors de la délivrance d'un certificat 14
2.1.2.2.1 Vérification de l'identité du demandeur lors de la remise du jeton d'initialisation 14
2.1.2.2.2 Vérification du jeton par l'application du service de certification 14
2.1.2.2.3 Vérification de la possession par l'abonné de sa clé privée 14
2.1.2.2.4 Vérification du bon fonctionnement de la clé privée 15

2.2 Vérification de l'identité avant le renouvellement d'un certificat 15

2.3 Vérification de l'identité avant la récupération d'un certificat 15
2.3.1 Vérification de l'identité du demandeur 15
2.3.2 Vérification du jeton par l'application du service de certification 16

2.4 Vérification de l'identité avant la suppression d'un certificat 16

2.5 Vérification de l'identité avant la rectification d'un certificat 16
2.5.1 Vérification de l'identité du demandeur 16

2.5.2 Vérification de la signature numérique du demandeur 16

2.6 Vérification de l'identité avant le retrait d'un certificat 16

3. PRATIQUES OPÉRATIONNELLES EN MATIÈRE DE DÉLIVRANCE ET D'OPÉRATIONS SUR LES CERTIFICATS 17

3.1 Règles de pratique à respecter lors de la délivrance d'un certificat 17
3.1.1 Individu pouvant demander la délivrance d'un certificat 17
3.1.2 Formulation du nom distinctif 17
3.1.2.1 Typologie des noms 17
3.1.2.2 Obligation d'utiliser un nom significatif 17
3.1.2.3 Unicité des noms 18
3.1.2.4 Règlement des différends concernant l'attribution des noms distinctifs 18
3.1.3 Procédure de demande de délivrance 18
3.1.4 Traitement d'une demande de délivrance 19
3.1.5 Délai de traitement d'une demande de délivrance 19
3.1.6 Acceptation et confirmation de la délivrance du certificat 19

3.2 Règles de pratique à respecter lors du renouvellement d'un certificat 19
3.2.1 Individus pouvant demander un renouvellement 19
3.2.2 Traitement d'une demande de renouvellement 19
3.2.3 Délai de traitement d'une demande de renouvellement 20
3.2.4 Confirmation de renouvellement 20
3.2.4.1 Confirmation à l'abonné du renouvellement de son certificat 20
3.2.4.2 Publication d'un certificat 20

3.3 Règles de pratique à respecter lors de la récupération d'un certificat 20
3.3.1 Individus pouvant demander une récupération 21
3.3.2 Traitement d'une demande de récupération 21
3.3.2.1 Récupération à la demande de l'abonné 21
3.3.2.2 Récupération à la demande d'un tiers 22
3.3.3 Délai de traitement d'une demande de récupération 22
3.3.4 Confirmation de la récupération 22
3.3.4.1 Confirmation à l'abonné de la récupération de son certificat 22
3.3.4.2 Publication d'un certificat 22

3.4 Règles de pratique à respecter lors de la révocation (annulation) d'un certificat 23
3.4.1 Personne pouvant procéder à la révocation 23
3.4.2 Traitement de la révocation 23
3.4.3 Délai de traitement de la révocation 23
3.4.4 Avis de révocation 23
3.4.4.1 Avis à l'abonné de la révocation de son certificat 23
3.4.4.2 Avis aux autres abonnés et utilisateurs de la révocation d'un certificat 24

3.5 Règles de pratique à respecter lors du retrait d'un certificat 24
3.5.1 Individu pouvant demander le retrait 24
3.5.2 Traitement d'une demande de retrait 24
3.5.3 Délai de traitement d'une demande de retrait 24
3.5.4 Confirmation du retrait 24
3.5.4.1 Confirmation à l'abonné du retrait de son certificat 24
3.5.4.2 Confirmation aux autres abonnés et utilisateurs du retrait d'un certificat 24

3.6 Règles de pratique à respecter lors de la rectification d'un certificat 24
3.6.1 Individus pouvant demander la rectification 24

3.6.2 Traitement d'une demande de rectification 25
3.6.3 Délai de traitement d'une demande de rectification....25
3.6.4 Confirmation d'une rectification 25
3.6.4.1 Confirmation à l'abonné de la rectification de son certificat....25
3.6.4.2 Publication d'un certificat....25

3.7 Règles de pratique à respecter lors de la suppression d'un certificat 25
3.7.1 Individus pouvant demander la suppression d'un certificat 25
3.7.2 Traitement d'une demande de suppression de certificat 25
3.7.3 Délai de traitement d'une demande de suppression de certificat....26
3.7.4 Confirmation de la suppression....26
3.7.4.1 Confirmation à l'abonné de la suppression de son certificat 26
3.7.4.2 Publication d'un certificat....26

3.8 Procédures de vérification de la sécurité informatique....26
3.8.1 Types d'événements enregistrés....26
3.8.2 Délai de conservation des journaux de vérification de la sécurité du service de certification....27
3.8.3 Mesures de protection des journaux de vérification de la sécurité du service de certification....27
3.8.4 Traitement des journaux de vérification de la sécurité du service de certification....27
3.8.5 Avis à la suite d'un événement critique 27
3.8.6 Évaluation de la vulnérabilité....27

3.9 Politique de sauvegarde (copies de sécurité)....28
3.9.1 Types de données sauvegardées 28
3.9.2 Conservation des copies de sécurité....28

3.10 Politique de conservation des données 28
3.10.1 Types de données conservées 28
3.10.2 Délai de conservation des données 28

3.11 Politique de changement des clés 29

3.12 Compromission de clé privée 29

3.13 Plan d'urgence 29

3.14 Cessation des opérations du service de certification 29

4. MESURES DE SÉCURITÉ....29

4.1 Mesures de sécurité concernant les lieux physiques 29
4.1.1 Mesures de sécurité physique pour le serveur du service de certification....29
4.1.2 Mesures de sécurité physique pour le serveur du répertoire 30
4.1.3 Mesures de sécurité physique pour certains postes de travail du service de certification 30
4.1.4 Mesures de sécurité physique pour le poste de l'AVI 30
4.1.5 Mesures de sécurité physique pour le poste de l'abonné....30

4.2 Mesures de sécurité concernant l'administration....31
4.2.1 Structure organisationnelle du service de certification....31
4.2.2 Nombre de personnes requises pour effectuer les tâches....31
4.2.3 Nombre de personnes autorisées à consulter le code de vérification d'identité....31

4.3 Mesures de sécurité concernant le personnel....31
4.3.1 Mesures de sécurité concernant le personnel du service de certification. 31
4.3.2 Vérification des antécédents et des qualifications....31

4.3.2.1 Processus de vérification des antécédents judiciaires 31
4.3.2.2 Processus de vérification des qualifications....32
4.3.3 Formation 32
4.3.3.1 Formation du personnel du service de certification....32
4.3.3.2 Fréquence des cours de rappel....32
4.3.4 Personnel contractuel....32
4.3.5 Documentation fournie au personnel....32

4.4 Mesures de sécurité concernant les AVI 32

4.5 Mesures de sécurité concernant les abonnés et les utilisateurs....33

4.6 Mesures de sécurité concernant la technologie 33
4.6.1 Génération et livraison des clés et des certificats 33
4.6.1.1 Génération des paires de clés 33
4.6.1.2 Livraison de la clé privée à son titulaire 33
4.6.1.3 Livraison de la clé publique au service de certification 33
4.6.1.4 Livraison à l'abonné de la clé publique du sceau du service de certification 34
4.6.1.5 Taille des clés 34
4.6.1.6 Génération matérielle/logicielle des clés....34
4.6.1.7 Génération des paramètres des certificats 34
4.6.1.8 Contrôle de la qualité des paramètres 34
4.6.1.9 Utilisation du champ d'extension « type d'utilisation de la clé » 34
4.6.1.10 Génération du certificat de l'abonné....34
4.6.1.11 Livraison du certificat à l'abonné....34
4.6.2 Protection de la clé privée et des codes d'accès....34
4.6.2.1 Protection de la clé privée de l'abonné....34
4.6.2.2 Protection de la clé privée du service de certification....35
4.6.2.3 Support des clés privées 35
4.6.2.4 Normes à respecter par les modules cryptographiques 35
4.6.2.5 Remise à un tiers de la clé privée 35
4.6.2.6 Sauvegarde de la clé privée 36
4.6.2.7 Conservation de la clé privée par le service de certification....36
4.6.2.8 Méthode d'activation de la clé privée....36
4.6.2.9 Méthode de désactivation de la clé privée....36
4.6.2.10 Méthode de destruction de la clé privée 36
4.6.3 Autres aspects de la gestion des paires de clés....36
4.6.3.1 Période de validité des clés publiques et des clés privées 36
4.6.3.2 Période de validité des certificats 37
4.6.4 Jeton d'initialisation....37
4.6.4.1 Génération des codes formant le jeton d'initialisation....37
4.6.4.2 Protection des codes formant le jeton d'initialisation 37
4.6.4.3 Transmission des codes formant le jeton d'initialisation....37
4.6.4.4 Installation des codes formant le jeton d'initialisation 37
4.6.5 Mesures de sécurité des ordinateurs....37
4.6.5.1 Exigences techniques particulières 37
4.6.6 Contrôle de l'évolution du service de certification 38
4.6.6.1 Mesures de contrôle du développement des systèmes 38
4.6.6.2 Niveau d'évaluation de l'évolution du service de certification....38

5. FORMAT ET CONTENU DES CERTIFICATS, DU RÉPERTOIRE ET DES LCA 39

5.1 Des certificats....39
5.1.1 Champ « version » 39
5.1.2 Champ « numéro de série » 40

5.1.3 Champ « émetteur » 40
5.1.4 Champ « validité » 40
5.1.5 Champ « sujet » 40
5.1.6 Champ d'extension « type d'utilisation de la clé » 40
5.1.7 Champ d'extension « numéro des politiques » 40
5.1.8 Champ d'extension « équivalence entre les numéros de politiques » 40
5.1.9 Champ d'extension « type de vérification des politiques » 40
5.1.10 Champ « code de raison » 40
5.1.11 Champs d'extension des LCA 40
5.1.12 Archivage des certificats d'un abonné 41

5.2 Du répertoire 41

5.3 De la LCA 41

5.4 Périodicité et mise à jour des certificats, du répertoire et de la LCA 41

5.5 Renseignements dont l'exactitude est confirmée 41

5.6 Limite à l'utilisation des certificats et du répertoire 42

6. ADMINISTRATION DES POLITIQUES 42

6.1 Procédures de modification 42
6.1.1 Avis de modification 42
6.1.2 Forme de diffusion des avis 42
6.1.3 Éléments qui requièrent de nouvelles politiques 42

6.2 Procédure de diffusion 42
6.2.1 Diffusion des politiques 42
6.2.2 Pratiques de certification 43
6.2.3 Contrôle de l'accès 43

6.3 Vérification de la conformité 43
6.3.1 Vérification de la conformité du service de certification 43
6.3.2 Vérification de la conformité de l'AVI 43
6.3.3 Vérification de la conformité des utilisateurs 44

7. DISPOSITIONS DIVERSES 44

7.1 Protection des renseignements personnels 44

7.2 Mécanismes de traitement des plaintes 44

7.3 Garanties et limites à la responsabilité 44

7.4 Tarifs 45

7.5 Interprétation et mise en application 45
7.5.1 Lois et règlements applicables 45
7.5.2 Règlement des différends 45
7.5.3 Indépendance des dispositions 45

Introduction

Le Registre des droits personnels et réels mobiliers (ci-après nommé le « RDPRM ») a été créé le 1er janvier 1994, date d'entrée en vigueur du *Code civil du Québec*. Sa mission est de publier les droits personnels et réels mobiliers de manière à les rendre opposables aux tiers. Cette mission s'inscrit dans un contexte de modernisation complète du système de publicité des droits.

Bien que le processus de décentralisation de l'information ait été amorcé dès l'implantation du Registre, ce dernier étant déjà accessible par téléphone, sur des écrans de consultation dans différents points de service, par courrier et par télécopieur, il devenait impératif dès 1997 de prendre le virage technologique et d'offrir la consultation et l'inscription au moyen d'outils de plus en plus utilisés par la clientèle.

Un des virages technologiques retenus par l'Officier de la publicité des droits personnels et réels mobiliers (ci-après nommé l'« Officier ») est de permettre à la clientèle du RDPRM de transmettre les réquisitions d'inscription au Bureau de la publicité des droits personnels et réels mobiliers par voie électronique, en autant que les réquisitions reçues par cette voie soient considérées comme intègres, intégrales, qu'elles ne puissent être répudiées, que la confidentialité des données contenues dans celles-ci et dans les demandes de services soit assurée et que l'expéditeur puisse exprimer son consentement par rapport au contenu de la réquisition.

Pour permettre la transmission des réquisitions par voie électronique, l'Officier a opté pour le concept d'infrastructure à clés publiques (ci-après nommée « ICP ») qui est actuellement le concept émergeant dans le domaine du commerce électronique. Il a donc créé l'ICP du RDPRM. Ce concept d'ICP implique que l'Officier ait recours à un prestataire de service de certification qui a comme fonction de gérer des certificats électroniques d'identité pour la signature numérique et pour la confidentialité. Il a également recours à un prestataire de service de répertoire dans lequel répertoire sont publiés les certificats publics de chiffrement ainsi que la LCA. Aux présentes, ces prestataires seront nommés « service de certification ». Les certificats servent à assurer l'intégrité, l'intégralité, la confidentialité, la non-répudiation de l'envoi ainsi que le consentement de l'expéditeur.

En matière de sécurité, l'Officier a établi les exigences qu'il requiert pour tous les processus entourant les activités du service de certification lesquels sont décrits dans les présentes politiques.

L'Officier considère que toutes les réquisitions transmises par voie électronique, en utilisant des clés et des certificats de signature et de confidentialité délivrés conformément aux présentes politiques, sont signées numériquement.

Les présentes politiques constituent donc un «énoncé de politique » au sens de l'article 52 de la *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., c. C-1.1).

1. Renseignements généraux

Ce chapitre indique notamment l'identification et le champ d'application des politiques ainsi que les différents types d'intervenants visés.

1.1 Identification

1.1.1 Nom des politiques

Les présentes politiques portent le nom de « Politiques de certificats de signature et de confidentialité du Registre des droits personnels et réels mobiliers ». L'expression certificats de confidentialité vise des certificats de chiffrement.

1.1.2 Identifiants d'objet

Les présentes politiques déterminent, pour chacun des types de certificats, un ensemble de règles qui lui sont applicables. Également chaque type de certificats est identifié par un numéro spécifique nommé « identifiant d'objet ».

Les identifiants d'objet pour les différents certificats pouvant être délivrés en vertu des présentes politiques sont les suivants :

Types de certificats	Identifiants d'objet
Certificat de signature d'un abonné qui est un individu	2.16.124.10.101.8.5.2.1.2.32
Sceau d'un abonné qui n'est pas un individu	2.16.124.10.101.8.5.2.1.2.31
Certificat de chiffrement d'un abonné qui est un individu	2.16.124.10.101.8.5.2.1.1.32
Certificat de chiffrement d'un abonné qui n'est pas un individu	2.16.124.10.101.8.5.2.1.1.31

1.2 Champ d'application des politiques

Les présentes politiques s'appliquent à tous les intervenants de l'ICP du RDPRM. L'utilisation des clés et certificats délivrés en vertu des présentes politiques est limitée à la transmission de documents par voie électronique au Bureau de la publicité des droits personnels et réels mobiliers ou l'expédition de tels documents par ce dernier.

Signature numérique	*Confidentialité*
Les certificats de signature sont prévus pour : • vérifier l'identité de l'expéditeur d'un envoi électronique; • manifester la volonté de l'expéditeur relativement aux envois électroniques; • vérifier l'intégrité des envois électroniques.	Les certificats de chiffrement sont prévus pour : • assurer la confidentialité des envois électroniques.

1.3 Coordonnées du responsable des présentes politiques

Officier de la publicité des droits personnels et réels mobiliers
Registre des droits personnels et réels mobiliers
Direction des registres et de la certification
Ministère de la Justice du Québec

1, rue Notre-Dame Est, 7e étage
Montréal (Québec) H2Y 1B6
Téléphone : (514) 864-4949 menu vocal option 3
Télécopieur : (514) 864-4867
Courrier électronique : services@infocles.justice.gouv.qc.ca
Sites Internet : www.rdprm.gouv.qc.ca
www.infocles.justice.gouv.qc.ca

1.4 Entente de reconnaissance

Une entente de reconnaissance peut être conclue avec un autre prestataire de service de certification afin de permettre l'utilisation des certificats de ce prestataire de service de certification. Cette entente est mutuelle, lorsque deux services de certification acceptent les certificats l'un de l'autre ou, unilatérale, lorsque la reconnaissance est seulement dans un sens.

1.5 Intervenants de l'ICP du RDPRM

1.5.1 Service de certification

Dans les présentes politiques, le service de certification est sous la responsabilité de l'Officier. Il est responsable de la délivrance des clés et des certificats utilisés pour les transactions électroniques effectuées entre le RDPRM et ses clients. Il a la responsabilité d'identifier ou de faire identifier les demandeurs, de délivrer des certificats à leur nom et d'apposer son sceau sur les certificats qu'il délivre pour en prouver l'authenticité et, par le fait même, prouver l'identité de l'abonné. Il a pour fonction d'administrer des équipements et des logiciels, d'assurer le contrôle et de sécuriser l'accès à toutes composantes de son organisation.

Le service de certification est donc responsable de l'ensemble des aspects opérationnels et technologiques associés à la délivrance des clés et des certificats et aux opérations subséquentes reliées à leur cycle de vie, à l'exception de la vérification de l'identité initiale de l'abonné, laquelle relève de l'agent de vérification de l'identité (ci-après nommé « AVI »).

Le service de certification se conformant aux présentes politiques a pour fonction de :

- planifier l'implantation et d'assurer l'entretien de l'infrastructure du service;
- coordonner les demandes de certificats électroniques d'identité;
- ouvrir et mettre à jour un dossier pour chaque abonné;
- garantir l'intégrité des certificats délivrés en y apposant son sceau;
- diffuser l'information sur les certificats annulés (retirés, révoqués);
- faire respecter les présentes politiques;
- gérer l'évolution du service.

Le service de certification doit notamment:

- se conformer aux présentes politiques;
- mettre à la disposition de l'Officier des documents explicatifs sur ses pratiques de certification.

1.5.2 AVI

L'AVI est :

- autorisé par l'Officier suivant les critères établis par celui-ci;
- reconnu par le service de certification.

L'AVI effectue la vérification initiale de l'identité d'un abonné; il a les responsabilités et obligations suivantes:

- respecter les exigences opérationnelles déterminées par l'Officier;
- vérifier l'identité des abonnés conformément aux présentes politiques;
- recueillir les renseignements requis par l'Officier et les lui transmettre selon les moyens que ce dernier détermine;
- protéger la confidentialité de tout renseignement personnel ou code de vérification;
- le cas échéant, conserver selon les lois applicables les renseignements recueillis dans le cadre de la vérification de l'identité et classer ces renseignements de manière à les retracer sur demande en tout temps;
- protéger ses équipements contre toute atteinte à leur sécurité et leur intégrité;
- se conformer à toutes les exigences des présentes politiques le concernant.

À défaut, le service de certification peut prendre toute mesure qui lui semble appropriée et l'Officier peut retirer à l'AVI l'autorisation d'agir à ce titre.

1.5.3 Abonné

Un abonné est un individu ou un dispositif à qui le service de certification a délivré des clés et des certificats dont les coordonnées sont inscrites dans le répertoire public. L'abonné ou le représentant d'un abonné qui n'est pas un individu doivent se conformer à toutes les exigences décrites dans les présentes politiques les concernant.

1.5.3.1 Abonné qui est un individu

L'individu dont le certificat porte le numéro d'identifiant d'objet des présentes politiques est autorisé par l'Officier à utiliser ses clés et certificats, selon les règles prévues à cet effet, pour transmettre des documents par voie électronique au RDPRM, pour son propre compte ou pour le compte d'autrui.

L'abonné a les responsabilités et obligations suivantes :

- fournir à l'AVI des renseignements exacts et produire des pièces ou documents pertinents;
- utiliser ses clés adéquatement pour les seules fins autorisées;
- protéger le jeton d'initialisation;
- assurer la sécurité et la confidentialité de ses clés privées et de son code de vérification. Le cas échéant, modifier son code de vérification à la demande du Service de certification;

- aviser le plus rapidement l'Officier, lorsque la sécurité ou la confidentialité d'une de ses clés privées est compromise;
- protéger ses équipements, par exemple vérifier que ses clés privées sont désactivées avant de quitter son poste de travail;
- ne pas utiliser une clé privée, lorsque le certificat correspondant est annulé ou suspendu;
- détruire ses clés, lorsqu'il ne les utilise plus ou ne peut plus les utiliser.

Il doit :

- être une personne physique.

1.5.3.2 Abonné qui n'est pas un individu (dispositif physique ou applicatif)

Seul le RDPRM ou un autre ministère ou organisme autorisé par l'Officier peut être un abonné qui n'est pas un individu.

L'individu responsable d'un abonné qui n'est pas un individu (dispositif) est responsable du certificat identifiant l'abonné.

L'individu responsable de cet abonné doit :

- être une personne physique dûment autorisée à détenir des clés et certificats au nom de l'abonné qui n'est pas un individu;
- fournir à l'AVI des renseignements exacts et produire des pièces ou documents pertinents;
- faire inscrire le nom de l'abonné qu'il représente dans les certificats. Ce nom doit préciser l'identification ou l'acronyme du RDPRM, du ministère ou de l'organisme autorisé par l'Officier à posséder de tels certificats;
- assurer la sécurité et la confidentialité de son code de vérification;
- utiliser ou permettre l'utilisation des clés et certificats que par une personne autorisée et aux seules fins autorisées;
- aviser rapidement l'Officier, lorsque la sécurité ou la confidentialité des clés privées est compromise;
- ne pas utiliser une clé privée, lorsque le certificat correspondant est annulé ou suspendu;
- détruire les clés du dispositif, lorsqu'elles ne sont plus utilisées.

1.5.4 Utilisateur de certificats

Un utilisateur est :

- un abonné du service de certification qui délivre des certificats en vertu des présentes politiques;
- un abonné d'un service de certification ayant signé une entente de reconnaissance avec l'Officier;
- celui qui agit en se fondant sur un certificat délivré en vertu des présentes politiques.

L'utilisateur doit se conformer à toutes les exigences des politiques le concernant.

L'utilisateur a notamment les responsabilités et obligations suivantes :

- vérifier la validité d'un certificat avant de l'utiliser, notamment en s'assurant que le certificat n'est pas périmé, annulé (retiré, révoqué) ou suspendu et qu'il ne comporte pas la mention «certificat

d'essai » ou toute autre mention de même nature indiquant qu'on ne peut raisonnablement s'y fier;

- vérifier la portée d'un certificat avant de l'utiliser, notamment en s'assurant que le type de certificat est approprié pour l'usage qu'il désire en faire;
- vérifier la signature du service de certification sur le certificat;
- utiliser les certificats à l'aide d'applications répondant aux exigences de l'Officier.

La vérification de la validité d'un certificat peut s'effectuer en direct en s'assurant de la fiabilité et de l'intégrité de l'information communiquée ou à l'aide de la LCA la plus récente. Si une autre forme de vérification est effectuée ou si la vérification du certificat est incomplète, l'utilisation du certificat est aux risques de l'utilisateur. Par ailleurs, lorsque ce dernier récupère une LCA à partir d'un répertoire, il doit vérifier le sceau apposé par le service de certification émetteur.

2. Pratiques en matière d'identification et de vérification de l'identité

Ce chapitre définit les exigences d'identification des demandeurs de certificats électroniques d'identité portant un numéro d'identifiant d'objet des présentes politiques. Il précise également ce que sont la délivrance et les opérations subséquentes sur les certificats.

2.1 Vérifications relatives à la délivrance d'un certificat

La délivrance correspond à la production d'un certificat pour un abonné.

2.1.1 Vérifications requises de l'AVI avant la délivrance d'un certificat

2.1.1.1 Obligation d'une rencontre physique

Le demandeur doit être identifié en personne par un AVI autorisé par l'Officier.

2.1.1.2 Vérification des pièces d'identité requises pour l'identification d'un demandeur

L'AVI doit vérifier deux pièces d'identité du demandeur émises par une autorité gouvernementale fédérale ou provinciale dont au moins une comporte sa photo et sa signature.

L'AVI doit prendre en note les types de pièces présentées et leur date d'émission ou d'expiration.

2.1.1.3 Vérification requises pour un abonné qui est un individu

2.1.1.3.1 Individu agissant pour son propre compte

L'abonné qui est un individu est aussi le demandeur. Son identité doit être vérifiée tel que décrit à la sous-section 2.1.1.

2.1.1.3.2 Individu agissant pour le compte d'autrui

L'AVI doit vérifier l'identité du demandeur tel que décrit à la sous-section 2.1.1.

Il doit également vérifier l'identification et l'existence du représenté, notamment par la vérification des informations publiées sur le registre prévu à la *Loi sur la publicité légale des entreprises individuelles, des sociétés et des personnes morales* (L.R.Q., c. P-45) ou par la vérification de tout autre document procurant une certitude équivalente.

L'AVI doit obtenir du demandeur un document attestant que ce dernier est autorisé à transmettre des documents par voie électronique au RDPRM pour le compte du représenté.

2.1.1.4 Vérification requises pour un abonné qui n'est pas un individu (dispositif)

L'AVI doit vérifier l'identité du responsable de l'abonné qui n'est pas un individu tel que décrit à la sous-section 2.1.1.

L'AVI doit également vérifier :

- l'identification et l'existence du RDPRM, du ministère ou de l'organisme lié à l'abonné;
- l'autorisation donnée au ministère ou à l'organisme par l'Officier pour l'obtention d'un tel type de certificats. À cette fin, le demandeur doit produire une lettre signée par l'Officier confirmant son autorisation;
- l'identification du dispositif auquel est affecté le certificat. À cette fin, le demandeur doit produire une déclaration signée par un représentant autorisé, selon le cas, du RDPRM, du ministère ou de l'organisme indiquant l'identification du dispositif visé;
- l'habilitation donnée au responsable par le RDPRM, le ministère ou l'organisme afin d'être titulaire d'un tel certificat. Cette vérification est faite par tout moyen jugé approprié par l'AVI, notamment par la consultation d'un document public (loi, décret, etc.) ou par l'obtention d'une déclaration signée par un représentant autorisé, selon le cas, du RDPRM, du ministère ou de l'organisme.

2.1.1.5 Compte rendu de la vérification de l'identité

L'AVI doit dresser et transmettre au service de certification un compte rendu de la vérification de l'identité selon les exigences opérationnelles de ce service.

Ce compte rendu doit comporter, notamment:

- le nom du demandeur, tel que vérifié suivant les prescriptions de la section 2.1;
- le fait que la vérification de l'identité a été faite en la présence physique du demandeur;
- les autres renseignements vérifiés par l'AVI, le cas échéant;
- l'intention du demandeur d'utiliser ses clés et certificats pour transmettre pour lui-même ou pour le compte d'autrui, par voie électronique, des documents au RDPRM, ou, dans le cas de dispositif, l'intention d'utiliser les clés et certificats dans le cadre d'échanges de documents avec le RDPRM;
- la date du compte rendu;
- le nom et la signature de l'AVI.

L'envoi d'un compte rendu comprend également le code de vérification choisi par le demandeur pour s'identifier auprès du service de certification. Cet envoi doit être signé et chiffré par l'AVI au moyen de clés qui offrent au moins le même degré de sécurité et de fiabilité que celles délivrées dans le cadre des présentes politiques.

2.1.2 Vérifications requises du service de certification avant la délivrance d'un certificat

2.1.2.1 Lors de la demande de délivrance d'un certificat

Lorsqu'un demandeur veut obtenir des clés et certificats et qu'il en a été titulaire dans l'année précédente, la vérification de son identité peut être faite à l'aide de son code de vérification s'il a l'intention de transmettre des documents au RDPRM pour son compte seulement.

Dans les autres cas, la vérification de l'identité doit être faite conformément à la sous-section 2.1.1.

2.1.2.2 Lors de la délivrance d'un certificat

2.1.2.2.1 Vérification de l'identité du demandeur lors de la remise du jeton d'initialisation

L'opération de téléchargement des clés et des certificats doit débuter par la saisie de deux codes qui ensemble forment le « jeton d'initialisation ».

À la suite de la réception et de l'acceptation d'un compte rendu de vérification, le service de certification transmet au demandeur la première partie du jeton d'initialisation.

Avant de remettre au demandeur la deuxième partie du jeton d'initialisation, le service de certification doit vérifier son identité à l'aide du code de vérification d'identité inscrit à son dossier. Lorsqu'il y a possibilité de compromission de ce code ou lorsque le demandeur n'est pas en mesure de le fournir, la remise de la deuxième partie du jeton d'initialisation ne peut être effectuée. La vérification de l'identité doit alors se faire de la manière décrite à la sous-section 2.1.1.

2.1.2.2.2 Vérification du jeton par l'application du service de certification

Lors d'une demande de délivrance, le service de certification doit vérifier que les deux parties du jeton transmises au demandeur et saisies par ce dernier pour obtenir ses certificats forment le jeton que le service de certification lui a émis. De plus, il s'assure que ce jeton n'a pas dépassé une durée de vie de 15 jours de la date d'émission de la première partie du jeton. À défaut de respecter ce délai, le service de certification peut transmettre à l'abonné, selon les circonstances, un nouveau jeton.

2.1.2.2.3 Vérification de la possession par l'abonné de sa clé privée

Signature numérique	*Confidentialité*
Le service de certification doit vérifier si l'abonné est en possession de la clé privée associée à la clé publique de signature qui a été inscrite dans son certificat.	Aucune exigence particulière.

2.1.2.2.4 Vérification du bon fonctionnement de la clé privée

Signature numérique	*Confidentialité*
L'abonné doit démontrer le bon fonctionnement de sa clé privée de signature.	Aucune exigence particulière.

2.2 Vérification de l'identité avant le renouvellement d'un certificat

Pour la sécurité, les clés doivent être modifiées quand leur date d'expiration approche. De nouvelles paires de clés et de nouveaux certificats sont créés.

Selon les conditions prévues dans les présentes politiques, le renouvellement peut se faire de manière automatique lors de l'établissement d'un lien électronique entre le poste de l'abonné et le serveur du service de certification. Lors de la communication, le serveur du service de certification détecte que la validité des clés expire prochainement et il procède alors au renouvellement.

Signature numérique	*Confidentialité*
Un certificat de signature est renouvelé lorsque la clé de signature est en voie d'expiration. Le service de certification doit vérifier l'identité du demandeur à partir de sa signature numérique créée par la clé privée de signature active. Lorsque la période de validité d'une clé est échue, le renouvellement est impossible. L'abonné doit alors procéder à une nouvelle demande de délivrance de certificat conformément à la section 2.1.	Un certificat de chiffrement est renouvelé lorsque la clé de chiffrement est en voie d'expiration ou est expirée. Pour le renouvellement d'une paire de clés de chiffrement, le service de certification doit valider l'identité du demandeur à partir d'une signature numérique créée par une clé privée de signature active. Lorsque la période de validité de la clé de signature est échue, le renouvellement est impossible. L'abonné doit alors procéder à une nouvelle demande de délivrance de certificat conformément à la section 2.1.

2.3 Vérification de l'identité avant la récupération d'un certificat

2.3.1 Vérification de l'identité du demandeur

Le service de certification doit vérifier l'identité de l'individu qui fait une demande de récupération à l'aide du code de vérification d'identité inscrit au dossier de l'abonné. Lorsqu'il y a possibilité de compromission de ce code ou lorsque le demandeur n'est pas en mesure de le fournir, la demande ne peut être acceptée. Le demandeur doit alors effectuer une nouvelle demande de délivrance de certificat et faire vérifier son identité de la manière décrite à la section 2.1.

2.3.2 Vérification du jeton par l'application du service de certification

Lors d'une demande de récupération, le service de certification doit vérifier que les deux parties du jeton transmises au demandeur et saisies par ce dernier pour obtenir ses certificats forment le jeton que le service de certification lui a émis.

2.4 Vérification de l'identité avant la suppression d'un certificat

La suppression consiste à enlever définitivement des répertoires du service de certification le certificat d'un abonné ainsi que les données qui le concernent. Le certificat ne peut être utilisé car il n'est plus disponible. Si l'abonné a déjà effectué une transaction avec son certificat, cette opération ne peut être effectuée; l'abonné devra alors choisir le retrait.

Le service de certification doit vérifier l'identité de l'individu qui fait une demande de suppression à l'aide du code de vérification d'identité inscrit au dossier de l'abonné. Lorsqu'il y a possibilité de compromission de ce code ou lorsque le demandeur n'est pas en mesure de le fournir, la demande ne peut être acceptée.

2.5 Vérification de l'identité avant la rectification d'un certificat

La rectification est utilisée lorsque les lettres ou chiffres ajoutés au nom de l'abonné pour rendre son nom distinctif et unique doivent être modifiés.

2.5.1 Vérification de l'identité du demandeur

Le service de certification doit vérifier l'identité de l'individu qui fait une demande de rectification à l'aide du code de vérification d'identité inscrit au dossier de l'abonné. Lorsqu'il y a possibilité de compromission de ce code ou lorsque le demandeur n'est pas en mesure de le fournir, la demande ne peut être acceptée. Le demandeur doit alors effectuer une nouvelle demande de délivrance de certificat et faire vérifier son identité de la manière décrite à la section 2.1. De nouvelles clés et de nouveaux certificats lui seront délivrés et les anciens seront annulés.

Lorsque la demande implique une modification dans le nom de l'abonné vérifié et déclaré par l'AVI dans un compte rendu, la demande ne peut être acceptée. Le demandeur doit alors effectuer une nouvelle demande de délivrance de certificat et faire vérifier son identité de la manière décrite à la section 2.1.

2.5.2 Vérification de la signature numérique du demandeur

Avant de procéder à distance à la rectification du certificat dans le poste de l'abonné, le service de certification doit vérifier que la signature numérique de l'abonné est valide.

2.6 Vérification de l'identité avant le retrait d'un certificat

Le retrait des certificats se fait, notamment dans les circonstances suivantes:

- lorsqu'un abonné ne nécessite plus leur utilisation;
- s'il croit qu'il n'est plus le seul à y avoir accès;
- lorsque le certificat devient obsolète;
- lorsque l'information contenue dans le certificat n'est plus exacte.

Le service de certification doit vérifier l'identité de l'individu qui fait une demande de retrait à l'aide du code de vérification d'identité inscrit au dossier de l'abonné. Lorsqu'il y a possibilité de compromission de ce code ou lorsque le demandeur n'est pas en mesure de le fournir, la demande ne peut être acceptée.

3. Pratiques opérationnelles en matière de délivrance et d'opérations sur les certificats

L'Officier reconnaît au service de certification qui a le droit d'utiliser les identifiants d'objet des présentes politiques dans les certificats qu'il délivre, le pouvoir d'effectuer la délivrance et les opérations qui suivent.

Le service de certification doit documenter les demandes relatives aux certificats, les conserver et faire signer (marque) les opérations concernant les certificats. De plus, lorsque la demande nécessite la délivrance de nouveaux certificats, le service de certification doit suggérer à l'abonné d'effectuer une copie de sécurité des nouveaux certificats.

3.1 Règles de pratique à respecter lors de la délivrance d'un certificat

3.1.1 Individu pouvant demander la délivrance d'un certificat

Peut demander la délivrance d'un certificat :

- un individu.

3.1.2 Formulation du nom distinctif

3.1.2.1 Typologie des noms

Le nom apparaissant au certificat d'un abonné doit être le nom distinctif.

3.1.2.2 Obligation d'utiliser un nom significatif

Si l'abonné est un individu, le nom de l'individu apparaissant au certificat doit correspondre à ses nom et prénom usuel.

Si l'abonné est un abonné qui n'est pas un individu, le nom apparaissant au certificat doit être un nom significatif. Il comprend le nom de l'abonné ainsi que le nom ou l'acronyme du ministère ou de l'organisme autorisé à posséder un tel certificat.

Le nom distinctif de l'abonné apparaissant aux certificats doit comprendre le nom divulgué par l'abonné et vérifié par l'AVI lors de la vérification de l'identité.

La preuve du droit d'utiliser un nom est à la charge de celui qui requiert ce nom dans le certificat.

3.1.2.3 Unicité des noms

Les noms distinctifs doivent être uniques pour tous les certificats délivrés par un service de certification.

Des lettres ou des chiffres doivent être ajoutés au nom de l'abonné inscrit dans le certificat de façon à pouvoir assurer l'unicité du nom distinctif.

3.1.2.4 Règlement des différends concernant l'attribution des noms distinctifs

Le service de certification a toute discrétion pour l'attribution des lettres ou chiffres ajoutés au nom de l'abonné pour assurer l'unicité de son nom distinctif.

3.1.3 Procédure de demande de délivrance

Signature numérique	*Confidentialité*
Le demandeur d'un certificat de signature doit compléter les procédures suivantes : • soumettre une demande; • faire vérifier son identité et fournir les pièces justificatives requises, le cas échéant; • fournir ses nom et prénom usuel; • générer une paire de clés et transmettre la clé publique au service de certification en respectant les exigences définies dans « IETF PKIX Certificate Management Protocol »; • démontrer au service de certification qu'il a une paire de clés qui fonctionne.	Le demandeur d'un certificat de chiffrement doit compléter les procédures suivantes : • soumettre une demande; • faire vérifier son identité et fournir les pièces justificatives requises, le cas échéant; • fournir ses nom et prénom usuel; • démontrer au service de certification que la paire de clés qu'il a reçue est une paire de clés qui fonctionne.
Le demandeur d'un certificat de signature pour un abonné qui n'est pas un individu doit : • soumettre une demande; • faire vérifier son identité et fournir les pièces justificatives requises; • fournir le nom de l'abonné ainsi que le nom ou l'acronyme du ministère ou de l'organisme autorisé à obtenir un tel certificat; • générer une paire de clés et transmettre la clé publique au service de certification en respectant les exigences définies dans « IETF PKIX Certificate Management Protocol »; • démontrer au service de certification que la paire de clés qu'il a reçue est une paire de clés qui fonctionne.	Le demandeur d'un certificat de chiffrement pour un abonné qui n'est pas un individu doit : • soumettre une demande; • faire vérifier son identité et fournir les pièces justificatives requises; • fournir le nom de l'abonné ainsi que le nom ou l'acronyme du ministère ou de l'organisme autorisé à obtenir un tel certificat; • démontrer au service de certification que la paire de clés qu'il a reçue est une paire de clés qui fonctionne.

3.1.4 Traitement d'une demande de délivrance

Le service de certification doit:

- vérifier l'identité du demandeur;
- effectuer la génération et la transmission du jeton d'initialisation;
- assister l'abonné pour la création de ses clés et certificats, le cas échéant;
- créer et transmettre le certificat de l'abonné;
- suggérer à l'abonné d'effectuer une copie de sécurité de ses clés et de ses certificats.

3.1.5 Délai de traitement d'une demande de délivrance

Le traitement d'une demande de délivrance doit débuter au plus tard la première journée ouvrable suivant la réception de la demande.

3.1.6 Acceptation et confirmation de la délivrance du certificat

En apposant sa signature sur le certificat de l'abonné, le service de certification signifie son approbation de la demande de délivrance du certificat.

Le service de certification doit publier les certificats de chiffrement qu'il délivre dans un répertoire que les utilisateurs peuvent consulter en ligne.

Par l'inscription d'un certificat de chiffrement au répertoire, le service de certification certifie qu'il a délivré un tel certificat à l'abonné et que celui-ci l'a accepté. À la suite de cette inscription, le service de certification certifie aussi qu'il a délivré un certificat de signature numérique à l'abonné et que ce dernier l'a accepté.

3.2 Règles de pratique à respecter lors du renouvellement d'un certificat

3.2.1 Individus pouvant demander un renouvellement

Peuvent demander le renouvellement d'un certificat :

- l'abonné;
- le responsable d'un abonné qui n'est pas un individu.

Si le renouvellement se fait automatiquement, la demande est implicite; elle est alors produite par le système de l'abonné.

3.2.2 Traitement d'une demande de renouvellement

Si la clé privée de signature de l'abonné est toujours active, le service de certification doit:

- vérifier l'identité du demandeur;
- effectuer le renouvellement;
- vérifier que le certificat a été renouvelé;
- révoquer (annuler) le certificat précédent et mettre à jour la LCA.

Si la clé privée de signature de l'abonné n'est plus active, le renouvellement ne peut avoir lieu et l'abonné doit demander la délivrance de nouveaux certificats conformément à la section 2.1.

3.2.3 Délai de traitement d'une demande de renouvellement

Si la demande n'est pas effectuée automatiquement, le traitement d'une demande de renouvellement doit débuter au plus tard la première journée ouvrable suivant la réception de la demande. Si la demande est effectuée automatiquement, elle est traitée à sa réception.

3.2.4 Confirmation de renouvellement

3.2.4.1 Confirmation à l'abonné du renouvellement de son certificat

Le service de certification doit informer l'abonné de la création de son certificat dans les trois jours ouvrables suivant le renouvellement.

3.2.4.2 Publication d'un certificat

Signature numérique	*Confidentialité*
Aucune exigence particulière.	Le service de certification doit publier le certificat renouvelé dans un répertoire qui est, sauf exception, disponible et accessible aux utilisateurs. En inscrivant un certificat de chiffrement dans le répertoire, le service de certification certifie qu'il a délivré un tel certificat à l'abonné et que ce dernier l'a accepté.

3.3 Règles de pratique à respecter lors de la récupération d'un certificat

Signature numérique	*Confidentialité*
Les certificats de signature ne sont jamais récupérés. L'action de récupérer des clés et des certificats de chiffrement engendre la création d'une nouvelle paire de clés de signature et d'un nouveau certificat de signature. Le certificat précédent est alors révoqué (annulé).	La récupération est un processus par lequel l'usage d'un certificat de chiffrement est recouvré. La récupération est utilisée dans certaines circonstances, par exemple lorsqu'un abonné a oublié le mot de passe donnant accès à son certificat ou en cas de bris, de dysfonctionnement ou de perte du support d'un tel certificat. Un certificat de chiffrement peut être récupéré à partir des données conservées au service de certification. Le service de certification retrouve dans ses bases de données le certificat de l'abonné qui demande une récupération et le lui retransmet. Cet abonné retrouve en même temps la clé privée de chiffrement correspondante.

3.3.1 Individus pouvant demander une récupération

Peuvent demander la récupération d'un certificat :

- l'abonné;
- le responsable d'un abonné qui n'est pas un individu;
- le responsable de l'accès aux documents des organismes publics ou de la protection des renseignements personnels nommé en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1);
- toute personne autorisée à demander la récupération à la suite d'un jugement ayant l'autorité de la chose jugée rendu par un tribunal compétent.

3.3.2 Traitement d'une demande de récupération

3.3.2.1 Récupération à la demande de l'abonné

Signature numérique	*Confidentialité*
Les certificats de signature ne sont jamais récupérés. L'action de récupérer des clés et des certificats de chiffrement engendre la création d'une nouvelle paire de clés de signature et d'un nouveau certificat de signature. Pour ce faire, le service de certification doit : • vérifier l'identité de l'abonné; • effectuer la génération et la transmission du jeton d'initialisation. Après que l'abonné ait généré ses clés, il doit transmettre la clé publique au service de certification en respectant les exigences définies dans « IETF PKIX Certificate Management Protocol » et doit démontrer au service de certification qu'il a une paire de clés qui fonctionne. Après réception de la clé publique, le service de certification génère et transmet un nouveau certificat à l'abonné. Le certificat précédent est alors révoqué (annulé).	Pour ce faire, le service de certification doit vérifier l'identité de l'abonné. Le service de certification récupère les clés et le certificat de chiffrement pour les retransmettre à l'abonné.

3.3.2.2 Récupération à la demande d'un tiers

Signature numérique	*Confidentialité*
Les certificats de signature ne sont jamais récupérés. L'action de récupérer des clés et du certificat de chiffrement engendre la création d'une nouvelle paire de clés et d'un nouveau certificat de signature que le service de certification révoque (annule).	Pour ce faire, le service de certification doit vérifier l'identité du tiers et la validité de la demande. Le service de certification doit aviser l'abonné de la demande de récupération, sauf indication contraire du tribunal. Le service de certification récupère les clés et le certificat pour les retransmettre au tiers dans un fichier accompagné des mots de passe permettant leur utilisation. Le service de certification efface de ses systèmes toute copie du fichier ainsi créé et révoque (annule) le certificat de chiffrement sur confirmation que les données ont été récupérées.

3.3.3 Délai de traitement d'une demande de récupération

Le traitement d'une demande de récupération doit débuter au plus tard la première journée ouvrable suivant la réception de la demande.

3.3.4 Confirmation de la récupération

3.3.4.1 Confirmation à l'abonné de la récupération de son certificat

Signature numérique	*Confidentialité*
Lorsque la demande de récupération est faite par l'abonné, le service de certification l'informe de la création de son nouveau certificat de signature dans les trois jours ouvrables suivant la récupération du certificat de chiffrement. Le service de certification doit conserver une trace de cette communication.	Sauf indication contraire du tribunal, le service de certification doit informer le demandeur de la récupération de son certificat dans les trois jours ouvrables suivant celle-ci. Le service de certification doit conserver une trace de cette communication.

3.3.4.2 Publication d'un certificat

Signature numérique	*Confidentialité*
Aucune exigence particulière.	Le certificat est déjà publié.

3.4 Règles de pratique à respecter lors de la révocation (annulation) d'un certificat

La révocation consiste à ne plus reconnaître la validité d'un certificat même si la date d'expiration n'est pas encore atteinte.

La révocation peut résulter des situations suivantes :

- s'il s'est écoulé une période de plus de six mois consécutifs sans que le titulaire n'utilise ses certificats;
- s'il y a des raisons de croire qu'un certificat est altéré;
- s'il y a des raisons de croire que la sécurité des clés ou des certificats est compromise;
- si le titulaire n'est plus autorisé à transmettre électroniquement des documents pour autrui au Bureau de la publicité des droits personnels et réels mobiliers;
- si le titulaire ne respecte pas ses obligations;
- si les renseignements mentionnés aux certificats ne sont plus exacts, notamment lors du changement de nom de l'abonné ou de l'entreprise pour laquelle il agit.

3.4.1 Personne pouvant procéder à la révocation

Seul le service de certification peut approuver la révocation et autoriser le déclenchement de la procédure de révocation.

3.4.2 Traitement de la révocation

Le service de certification doit :

- effectuer la suspension. Cette dernière consiste à rendre temporairement inaccessible le certificat d'un abonné. Sans être révoqué (annulé), le certificat ne peut plus être utilisé car il n'est pas disponible;
- analyser les faits pouvant entraîner la révocation;
- effectuer, s'il y a lieu, la révocation ou la réactivation;
- informer l'abonné;
- vérifier que le certificat a été révoqué;
- mettre à jour la LCA.

Le certificat est révoqué (annulé) lorsqu'il est placé dans la LCA.

3.4.3 Délai de traitement de la révocation

Le traitement de la révocation par le service de certification doit débuter dès que celui-ci a connaissance de la survenance de l'une des situations entraînant la révocation.

3.4.4 Avis de révocation

3.4.4.1 Avis à l'abonné de la révocation de son certificat

Le service de certification doit informer l'abonné de la suspension et, s'il y a lieu, de la révocation de son certificat. Cet avis doit prendre la forme d'un courriel ou d'une lettre transmis à l'abonné. Le service de certification doit conserver une trace de cette communication.

3.4.4.2 Avis aux autres abonnés et utilisateurs de la révocation d'un certificat

Les autres abonnés et utilisateurs sont informés de la révocation par le fait que le certificat révoqué est mentionné dans la LCA.

3.5 Règles de pratique à respecter lors du retrait d'un certificat

3.5.1 Individu pouvant demander le retrait

Peuvent demander le retrait d'un certificat :

- l'abonné;
- le responsable d'un abonné qui n'est pas un individu.

3.5.2 Traitement d'une demande de retrait

Le service de certification doit :

- vérifier l'identité du demandeur;
- vérifier le bien fondé de la demande;
- effectuer le retrait;
- vérifier que le certificat a été retiré;
- mettre à jour la LCA.

3.5.3 Délai de traitement d'une demande de retrait

Le traitement d'une demande de retrait doit débuter au plus tard la première journée ouvrable qui suit la réception de la demande.

3.5.4 Confirmation du retrait

3.5.4.1 Confirmation à l'abonné du retrait de son certificat

Le service de certification doit informer l'abonné concerné du retrait de son certificat. Le service de certification doit conserver une trace de cette communication.

3.5.4.2 Confirmation aux autres abonnés et utilisateurs du retrait d'un certificat

Les autres abonnés et utilisateurs sont informés du retrait par le fait que le certificat retiré est mentionné dans la LCA.

3.6 Règles de pratique à respecter lors de la rectification d'un certificat

La rectification demande l'intervention du service de certification. Dès que les changements sont faits, la rectification s'effectue de manière automatique lors d'une communication établie entre le poste de l'abonné et le serveur du service de certification. Un nouveau certificat est alors créé et le certificat précédent est révoqué (annulé).

3.6.1 Individus pouvant demander la rectification

Peuvent demander la rectification d'un certificat :

- l'abonné;

- le responsable d'un abonné qui n'est pas un individu;
- les employés du service de certification.

3.6.2 Traitement d'une demande de rectification

Le service de certification doit :
- vérifier l'identité de l'abonné;
- vérifier le bien fondé de la demande;
- effectuer la rectification;
- vérifier que le certificat a été rectifié;
- annulé le certificat précédent et mettre à jour la LCA.

3.6.3 Délai de traitement d'une demande de rectification

Le traitement d'une demande de rectification doit débuter au plus tard la première journée ouvrable qui suit la réception de la demande.

3.6.4 Confirmation d'une rectification

3.6.4.1 Confirmation à l'abonné de la rectification de son certificat

Le service de certification doit informer l'abonné de la rectification de son certificat dans les trois jours ouvrables suivant celle-ci. Le service de certification doit conserver une trace de cette communication.

3.6.4.2 Publication d'un certificat

Signature numérique	*Confidentialité*
Aucune exigence particulière.	Le service de certification doit publier le certificat rectifié dans un répertoire qui est, sauf exception, disponible et accessible aux utilisateurs. En inscrivant un certificat de chiffrement dans le répertoire, le service de certification certifie qu'il a délivré un tel certificat à l'abonné et que ce dernier l'a accepté.

3.7 Règles de pratique à respecter lors de la suppression d'un certificat

3.7.1 Individus pouvant demander la suppression d'un certificat

Peuvent demander la suppression d'un certificat :
- l'abonné;
- le responsable d'un abonné qui n'est pas un individu;
- les employés du service de certification si l'abonné l'avait préalablement autorisé.

3.7.2 Traitement d'une demande de suppression de certificat

Le service de certification doit :

- vérifier l'identité du demandeur;
- vérifier le bien fondé de la demande;
- effectuer la suppression du certificat;
- vérifier que le certificat a été supprimé;
- demander à l'abonné de détruire ses clés.

3.7.3 Délai de traitement d'une demande de suppression de certificat

Le traitement d'une demande de suppression de certificat doit débuter au plus tard la première journée ouvrable suivant la réception de la demande.

3.7.4 Confirmation de la suppression

3.7.4.1 Confirmation à l'abonné de la suppression de son certificat

Le service de certification doit informer l'abonné de la suppression de son certificat dans les trois jours ouvrables suivant celle-ci. Le service de certification doit conserver une trace de cette communication.

3.7.4.2 Publication d'un certificat

Signature numérique	*Confidentialité*
Aucune exigence particulière.	Le service de certification doit supprimer le certificat du répertoire public.

3.8 Procédures de vérification de la sécurité informatique

3.8.1 Types d'événements enregistrés

Tous les événements pertinents relatifs à la sécurité du système du service de certification doivent être enregistrés dans les journaux de vérification de la sécurité de ce dernier, notamment les tentatives fructueuses ou non de :

- créer, modifier, enlever, désactiver, activer, réactiver, interdire ou récupérer les autorisations et les attributs des opérateurs de l'application et du système d'exploitation du serveur du service;
- créer, enlever, utiliser, mettre, remettre ou changer les mots de passe du service;
- créer, mettre à jour, révoquer, suspendre ou récupérer les clés et les certificats du service, de son personnel ou des abonnés;
- changer les paramètres de sécurité du système d'exploitation du serveur et de l'application du service;
- démarrer et arrêter l'application du service ainsi que les sessions et le système d'exploitation du serveur du service;
- établir une connexion ou écrire au répertoire par l'application du service;
- modifier les listes de tentative d'atteinte à la sécurité du service;
- modifier les bases de données du service.

Les renseignements suivants doivent aussi être retenus, documentés et conservés :

- les changements de l'architecture du service;
- les changements des paramètres relatifs à la création des certificats;
- la mise à jour du matériel informatique et des logiciels;
- les relevés d'activités d'entretien du système et du lieu physique du service et de ses systèmes;
- les accès physiques aux locaux du service;
- les changements de personnel;
- les rapports de non-conformité et de compromission;
- les ententes de reconnaissance;
- la correspondance officielle notamment celle relative aux intervenants de l'ICP et celle concernant les autres services de certification avec lesquels une entente de reconnaissance a été conclue;
- la destruction de tout support contenant des clés, des jetons ou de tout renseignement personnel ou confidentiel.

3.8.2 Délai de conservation des journaux de vérification de la sécurité du service de certification

Ces journaux doivent être conservés dans les locaux abritant le serveur du service de certification pour une période minimale de deux (2) mois. Après cette période, les données de ces journaux peuvent être conservées tel que décrit à l'article 3.10.2.

3.8.3 Mesures de protection des journaux de vérification de la sécurité du service de certification

Ces journaux doivent être protégés :

- en horodatant individuellement les entrées des listes;
- en horodatant les fichiers contenant les listes;
- en apposant la signature d'un membre autorisé du personnel du service de certification ou le sceau du service sur les fichiers.

3.8.4 Traitement des journaux de vérification de la sécurité du service de certification

Les journaux doivent être traités au moins une fois par semaine afin de :

- vérifier les listes de la semaine précédente;
- faire enquête sur les anomalies détectées et prendre les mesures nécessaires pour les résoudre;
- conserver les listes selon les modalités prévues aux présentes politiques.

3.8.5 Avis à la suite d'un événement critique

Dès qu'un événement interne à l'application met en péril l'intégrité du service de certification, l'application de ce service doit le signaler.

3.8.6 Évaluation de la vulnérabilité

Le service de certification doit, lors du traitement de toute information relative à un évènement relié à la sécurité colligée, prendre les mesures appropriées afin d'éliminer ou de réduire la vulnérabilité des systèmes.

3.9 Politique de sauvegarde (copies de sécurité)

3.9.1 Types de données sauvegardées

Les applications, les données et les fichiers suivants doivent être sauvegardés :

- les disques d'installation des systèmes d'exploitation;
- les disques d'installation de l'application du service de certification;
- les disques d'installation de l'application du répertoire;
- l'historique des clés et des certificats ainsi que la LCA;
- les données des répertoires;
- les renseignements pertinents sur les abonnés;
- les journaux de vérification de la sécurité du service de certification.

3.9.2 Conservation des copies de sécurité

Le service de certification doit conserver, dans un site sécuritaire, les copies des disques d'installation mentionnés à la sous-section 3.9.1 tant qu'il n'y a pas de nouvelles versions des produits concernés d'installées en production et pleinement opérationnelles.

De plus, il doit conserver une copie de sécurité des autres types de données mentionnés à ladite sous-section selon les périodes suivantes :

- quotidiennes (jour ouvrable) pendant au minimum une (1) semaine;
- hebdomadaires pendant au minimum un (1) mois;
- mensuelles pendant au minimum douze (12) mois.

Lorsque requis, ces copies permettent de récupérer les données perdues.

3.10 Politique de conservation des données

3.10.1 Types de données conservées

Les données et fichiers suivants doivent être conservés :

- toutes les données de vérification telles que décrites à la sous-section 3.8.1;
- tous les certificats et LCA générés;
- l'historique des clés;
- toute information pertinente sur les abonnés.

3.10.2 Délai de conservation des données

Les données relatives aux clés et aux certificats, aux abonnés ainsi que la correspondance officielle doivent être conservées pour une période minimale de 10 ans. Les données des journaux de vérification de la sécurité du service de certification doivent être conservées au moins deux ans.

3.11 Politique de changement des clés

Signature numérique	*Confidentialité*
Le renouvellement automatique des clés publiques et privées de signature doit débuter de deux à six mois avant la date d'expiration de la période de validité de la clé privée de signature.	Le renouvellement automatique des clés publiques et privées de chiffrement doit débuter de deux à six mois avant la date d'expiration de la période de validité de la clé publique de chiffrement.

3.12 Compromission de clé privée

Les procédures à suivre lors de la compromission de la clé privée du service de certification et de son personnel doivent être documentées. L'abonné est tenu d'aviser, dans les plus brefs délais, le service de certification de la compromission présumée ou avérée de sa clé privée.

3.13 Plan d'urgence

En cas de désastre, les plans de recouvrement des équipements et des logiciels du service de certification doivent être documentés. Notamment, ce plan de recouvrement doit prévoir les moyens qui seront mis en place afin que le service de certification soit de nouveau opérationnel dans les 48 heures qui suivent le moment où le désastre est survenu.

De plus, le service de certification doit effectuer des tests de reprise de ses services au minimum une fois par année.

3.14 Cessation des opérations du service de certification

Dans le cas où le service de certification cesserait ses opérations, il doit informer par écrit ses abonnés, les AVI faisant affaires avec lui ainsi que le service de certification avec qui il est lié par une entente de reconnaissance.

Si requis, les certificats délivrés par le service de certification peuvent être annulés. Dans un tel cas, une LCA devra être publiée.

4. Mesures de sécurité

4.1 Mesures de sécurité concernant les lieux physiques

4.1.1 Mesures de sécurité physique pour le serveur du service de certification

Le serveur du service de certification est localisé dans une zone de sécurité conforme aux normes suivantes :

- murs de plaquo-plâtre ou de contre-plaqué allant du vrai plancher au vrai plafond ou au plafond suspendu avec système de détection d'intrusion au-dessus du plafond suspendu;
- fenêtres et ouvertures de service obstruées par un grillage ou par un laminé ou un autre mécanisme anti-intrusion;
- fenêtres et ouvertures de service obstruées ne permettant pas de voir les écrans d'ordinateur à l'intérieur du local;

- porte avec verrou de sécurité et munie de dispositif permettant le contrôle des entrées;
- accès à la zone uniquement possible d'une autre zone à accès contrôlé et non d'une zone à accès publique;
- système de surveillance actif en absence du personnel autorisé ou système de détection d'intrusion lorsque la surveillance n'est pas possible;
- panneau indiquant « Zone à accès contrôlé – Personnel autorisé seulement » affiché de façon proéminente sur les portes d'accès;
- alimentation électrique d'appoint rencontrant les normes de protection contre le feu du ministère et du gouvernement;
- climatisation de la zone suffisante aux besoins des ordinateurs s'y trouvant et rencontrant les normes de protection contre le feu du gouvernement et du ministère;
- procédure documentée de destruction des documents sensibles et des supports contenant de tels documents.

L'accès au serveur est limité aux personnes autorisées par le service de certification et les entrées et sorties sont documentées. Toute autre personne doit être escortée et surveillée par une personne autorisée.

4.1.2 Mesures de sécurité physique pour le serveur du répertoire

Les mesures de sécurité physique en vigueur pour le serveur du répertoire doivent être similaires à celles du serveur du service de certification décrites à la sous-section 4.1.1.

4.1.3 Mesures de sécurité physique pour certains postes de travail du service de certification

Les mesures de sécurité physique pour contrôler l'accès aux postes de travail du personnel du service de certification affecté au traitement des comptes rendus de vérification doivent être similaires à celles du serveur du service de certification décrites à la sous-section 4.1.1.

L'accès réseau entre ces postes et les serveurs du service de certification doit se faire par un segment isolé.

4.1.4 Mesures de sécurité physique pour le poste de l'AVI

Lorsque l'AVI utilise un poste portatif, il doit en garder le contrôle en tout temps. Ce contrôle peut être effectué par des moyens physiques ou logiques.

L'AVI doit empêcher l'utilisation de son poste de travail lorsque ses clés privées sont actives.

L'information sensible emmagasinée sur le poste de l'AVI doit être protégée par des mesures de contrôle de l'activation du poste ou par chiffrement, de manière à préserver la confidentialité et l'intégrité des données concernant les abonnés.

4.1.5 Mesures de sécurité physique pour le poste de l'abonné

L'abonné doit empêcher l'utilisation de son poste de travail lorsque ses clés privées sont actives.

4.2 Mesures de sécurité concernant l'administration

4.2.1 Structure organisationnelle du service de certification

Afin de se prémunir contre toute personne qui pourrait porter préjudice à la sécurité et à l'intégrité du service de certification, ce dernier doit s'assurer que les fonctions liées à des tâches essentielles soient réparties entre plusieurs personnes. Le service de certification doit au minimum faire en sorte que les fonctions opérationnelles soient assumées par des membres de son personnel qui soient différents de ceux assumant les fonctions de vérification. Une personne ne peut occuper simultanément ces deux rôles.

4.2.2 Nombre de personnes requises pour effectuer les tâches

Deux personnes faisant partie du service de certification doivent collaborer pour effectuer les tâches suivantes :

- identifier et modifier la période de validité des clés;
- identifier et modifier la période de validité de la LCA;
- identifier et modifier les identifiants d'objets;
- créer, modifier, enlever, désactiver, activer, réactiver, interdire ou récupérer les autorisations et les attributs du personnel du service;
- mettre à jour la clé maîtresse du service de certification.

4.2.3 Nombre de personnes autorisées à consulter le code de vérification d'identité

Un nombre limité de membre du personnel du service de certification est autorisé à consulter les codes de vérification d'identité choisis par les abonnés pour la vérification de leur identité sans rencontre physique.

4.3 Mesures de sécurité concernant le personnel

4.3.1 Mesures de sécurité concernant le personnel du service de certification.

L'accomplissement des tâches par le personnel du service de certification doit être vérifié par leur responsable. Le personnel doit :

- remplir uniquement les fonctions décrites dans les présentes politiques ou remplir des fonctions décrites dans les présentes politiques et des fonctions qui ne rentrent pas en conflit avec celles du service de certification;
- remplir les fonctions qu'il est autorisé à exécuter;
- avoir complété un programme de formation portant sur les fonctions à remplir;
- posséder les qualifications nécessaires.

4.3.2 Vérification des antécédents et des qualifications

4.3.2.1 Processus de vérification des antécédents judiciaires

Les antécédents du personnel du service de certification ou des postulants à un emploi au service de certification doivent être vérifiés. Le service de certification doit vérifier que ces personnes

n'ont pas été déclarées coupables d'une infraction pénale ou criminelle ayant un lien avec l'emploi. Cette vérification doit être faite au moins une fois par année.

4.3.2.2 Processus de vérification des qualifications

Le service de certification vérifie la scolarité et les qualifications des postulants à un emploi au service de certification.

4.3.3 Formation

4.3.3.1 Formation du personnel du service de certification

Le personnel du service de certification doit poursuivre un programme de formation pertinent avant l'accomplissement de ses fonctions portant notamment sur :

- les normes juridiques et les exigences opérationnelles;
- les différentes applications et versions d'applications auxquelles il pourrait avoir accès;
- le matériel et les systèmes d'exploitation formant l'environnement opérationnel du service;
- les normes en matière de sécurité;
- la relève du service de certification après un sinistre, le cas échéant.

4.3.3.2 Fréquence des cours de rappel

Le personnel du service de certification doit participer à des séances de formation au besoin.

4.3.4 Personnel contractuel

Les mesures de sécurité ainsi que les exigences en matière d'antécédents judiciaires et des qualification spécifiées à la section 4.3 sont les mêmes quel que soit le lien contractuel unissant la personne au service de certification.

4.3.5 Documentation fournie au personnel

Le personnel du service de certification doit avoir accès à la documentation relative à ses responsabilités. Cette documentation doit porter sur les procédures habituelles telles que :

- la création des certificats;
- le renouvellement des certificats;
- l'annulation des certificats.

4.4 Mesures de sécurité concernant les AVI

L'AVI doit :

- avoir reçu la formation prescrite pour accomplir ses tâches;
- n'effectuer aucune autre tâche qui risque de le placer en conflit d'intérêts avec les tâches qui lui incombent en vertu des présentes politiques;
- respecter les normes d'éthique et de discipline relatives à son ordre professionnel.

4.5 Mesures de sécurité concernant les abonnés et les utilisateurs

Les abonnés et utilisateurs doivent connaître les pratiques de sécurité pertinentes à la protection de leur poste de travail et à leur module cryptographique. Le service de certification doit diffuser ces pratiques.

4.6 Mesures de sécurité concernant la technologie

Cette section contient les dispositions des politiques de gestion des paires de clés du service de certification, du personnel du service de certification et des abonnés.

4.6.1 Génération et livraison des clés et des certificats

4.6.1.1 Génération des paires de clés

Signature numérique	*Confidentialité*
La génération de la paire de clés de signature des abonnés doit se faire sur leur propre poste de travail ou sur le poste d'initialisation du service de certification. Les paires de clés de signature du personnel du service de certification qui sont conservées sur un support physique, telle une carte PCMCIA (Personnal Computer Memory Card International Association), doivent être générées à partir du poste d'initialisation du service de certification ou d'équipement autorisé par ce dernier.	Aucune exigence particulière

4.6.1.2 Livraison de la clé privée à son titulaire

Signature numérique	*Confidentialité*
La clé privée étant générée sur le poste de l'abonné, elle n'a pas à être livrée.	La clé privée de déchiffrement de l'abonné doit lui être livrée par une transaction en direct, conformément aux exigences définies dans le « IETF PKIX Certificate Management Protocol ».

4.6.1.3 Livraison de la clé publique au service de certification

Signature numérique	*Confidentialité*
La clé publique du sceau du service de certification doit lui être livrée par une transaction en direct, conformément aux exigences définies dans le « IETF PKIX Certificate Management Protocol ».	La clé publique de chiffrement étant générée par le service de certification, elle n'a pas à lui être livrée.

4.6.1.4 Livraison à l'abonné de la clé publique du sceau du service de certification

La clé publique du sceau du service de certification doit être livrée à l'abonné par une transaction en direct conformément aux exigences définies dans le «IETF PKIX Certificate Management Protocol ».

4.6.1.5 Taille des clés

Chaque clé d'une paire de clés doit être au moins de taille égale à 1024 bits selon l'algorithme RSA.

4.6.1.6 Génération matérielle/logicielle des clés

Les clés des abonnés et du personnel du service de certification doivent être générées sur un support matériel ou logiciel.

4.6.1.7 Génération des paramètres des certificats

Tous les paramètres nécessaires doivent être fournis par le service de certification.

4.6.1.8 Contrôle de la qualité des paramètres

Les paramètres utilisés lors de la génération des certificats doivent être conformes aux normes internationales reconnues.

4.6.1.9 Utilisation du champ d'extension « type d'utilisation de la clé »

Le champ « type d'utilisation de la clé » prévu dans les certificats de type X.509 doit obligatoirement être utilisé et ce, conformément à la norme X.509.

4.6.1.10 Génération du certificat de l'abonné

Le certificat de l'abonné doit être généré par le service de certification et un sceau garantissant l'intégrité du certificat doit être apposé par celui-ci.

4.6.1.11 Livraison du certificat à l'abonné

Le certificat de l'abonné doit lui être transmis en respectant les exigences définies dans « IETF PKIX Certificate Management Protocol ».

4.6.2 Protection de la clé privée et des codes d'accès

4.6.2.1 Protection de la clé privée de l'abonné

Les clés privées de chiffrement sont conservées par le service de certification; celles-ci doivent être protégées selon les modalités des présentes politiques.

L'abonné qui est un individu doit utiliser lui-même ses clés privées ainsi que le mot de passe y donnant accès. En aucun cas, il ne peut divulguer son code de vérification d'identité servant à s'identifier auprès du service de certification.

L'individu responsable d'un abonné qui n'est pas un individu peut permettre à des personnes autorisées d'utiliser la clé privée ainsi que le mot de passe y donnant accès. Cependant, en aucun cas, il ne peut divulguer son code de vérification d'identité servant à s'identifier auprès du service de certification.

Les personnes susmentionnées doivent prendre les précautions raisonnables pour en empêcher la modification, l'utilisation non autorisée, la divulgation, la perte ou le vol.

Si une clé privée est conservée chiffrée sur une disquette ou un autre support facilement transportable, ce support doit être conservé dans un lieu à accès contrôlé, lorsque non utilisé.

4.6.2.2 Protection de la clé privée du service de certification

Les mesures de sécurité stipulées dans les présentes politiques forment l'ensemble des mesures qui assurent la protection de la clé privée du service de certification.

4.6.2.3 Support des clés privées

Le personnel du service de certification, les abonnés qui sont des individus et les individus responsables des abonnés qui ne sont pas des individus qui maintiennent leur clé privée sur un support externe et transportable doivent choisir parmi les suivants :

- disquette (si une copie de sauvegarde est effectuée, elle est conservée tel qu'il est stipulé dans les présentes politiques);
- carte à puce;
- PCMCIA-II pouvant être validé au niveau 2 de FIPS PUB 140-1 et rencontrant les normes de PKCS#11
- tout autre support autorisé par l'Officier.

Le personnel du service de certification, qui doivent s'authentifier auprès de l'application de ce service à partir d'un réseau partagé ou d'un réseau public, doivent maintenir leur clé privée sur un support de type PCMCIA II pouvant être validé au niveau 2 de FIPS PUB 140-1 et rencontrant les normes de PKCS#11.

4.6.2.4 Normes à respecter par les modules cryptographiques

Toutes les opérations cryptographiques du service de certification doivent être effectuées à l'aide de logiciels cryptographiques classés au minimum FIPS 140-1 niveau 2.

Toutes les opérations cryptographiques des abonnés et du personnel du service de certification doivent être effectuées à l'aide de matériels ou logiciels cryptographiques classés FIPS 140-1 niveau 1 ou 2.

4.6.2.5 Remise à un tiers de la clé privée

Signature numérique	*Confidentialité*
Les clés privées de signature doivent être conservées uniquement par leur détenteur.	Si la clé privée de chiffrement doit être divulguée à une tierce partie, le consentement préalable de l'abonné doit être obtenu, sauf dans le cas où une loi ou un tribunal le requiert.

4.6.2.6 Sauvegarde de la clé privée

Si le support de la clé privée est une disquette, une copie de sauvegarde peut être prise et conservée dans un lieu à accès contrôlé.

4.6.2.7 Conservation de la clé privée par le service de certification

Signature numérique	*Confidentialité*
La clé privée de signature n'est pas connue du service de certification; il ne peut donc pas offrir le service de conservation pour cette clé.	Les clés privées de déchiffrement emmagasinées par le service de certification doivent être conservées selon les modalités de la présente politique.

4.6.2.8 Méthode d'activation de la clé privée

Les clés doivent être activées notamment par la saisie du mot de passe de l'abonné ou d'une mesure biométrique.

Lorsqu'un mot de passe est utilisé, cette donnée doit être imprévisible et soumise aux règles de sélection minimales suivantes :

- elle doit comporter un minimum de huit caractères;
- elle doit être constituée d'une combinaison de lettres majuscules, de lettres minuscules et de chiffres;
- elle ne doit pas contenir plus de quatre fois le même caractère.

Les abonnés doivent avoir la possibilité de changer leur mot de passe.

Le blocage du module cryptographique de l'abonné doit s'effectuer après trois tentatives infructueuses d'activation.

4.6.2.9 Méthode de désactivation de la clé privée

Les clés doivent être désactivées au moment de la fermeture de l'application et après une période prédéterminée d'inactivité de cette application n'excédant pas quinze minutes.

4.6.2.10 Méthode de destruction de la clé privée

Lorsqu'une clé privée n'est plus utilisée, toutes les copies de cette clé doivent être détruites de façon sécuritaire et de manière à ce que les données soient irrécupérables.

4.6.3 Autres aspects de la gestion des paires de clés

4.6.3.1 Période de validité des clés publiques et des clés privées

Signature numérique	*Confidentialité*
Pour les abonnés, la clé privée utilisée pour signer les envois électroniques doit être valide pour une période ne dépassant pas trois ans. La clé publique utilisée pour la vérification de la signature numérique doit être valide pour un	La clé privée de chiffrement doit être valide à perpétuité. Pour les abonnés, la clé publique utilisée pour le chiffrement des envois électroniques doit être valide pour un maximum de trois ans.

Signature numérique	*Confidentialité*
maximum de trois ans.	

4.6.3.2 Période de validité des certificats

Les certificats doivent être valides pour un maximum de trois ans.

4.6.4 Jeton d'initialisation

4.6.4.1 Génération des codes formant le jeton d'initialisation

Le pouvoir de générer les codes formant le jeton d'initialisation doit être attribué uniquement au service de certification.

4.6.4.2 Protection des codes formant le jeton d'initialisation

Les codes formant le jeton d'initialisation doivent être tenus séparés en tout temps à moins d'être dans le local abritant le serveur du service de certification. Dans ce dernier cas, les codes doivent être accessibles uniquement au service de certification et hors de la vue de toute autre personne.

4.6.4.3 Transmission des codes formant le jeton d'initialisation

Les codes formant le jeton d'initialisation doivent être transmis séparément au demandeur.

4.6.4.4 Installation des codes formant le jeton d'initialisation

La réunion des deux codes doit se faire uniquement par le demandeur.

4.6.5 Mesures de sécurité des ordinateurs

4.6.5.1 Exigences techniques particulières

Le serveur du service de certification doit être conforme aux exigences suivantes:

- protection du serveur du service de certification par un bastion;
- contrôle de l'accès au service de certification et aux autorisations et attributs du personnel du service;
- séparation forcée des pouvoirs du personnel du service de certification;
- identification et vérification de l'identité du personnel du service;
- processus de ré-initialisation obligatoire des objets contenus dans la mémoire vive ou le disque rigide du serveur du service de certification avant leurs réutilisations;
- utilisation du chiffrement pour les sessions de communication et la sécurité des bases de données sensibles;
- conservation de l'historique des clés du service de certification et de ses abonnés;
- conservation des journaux de vérification de la sécurité du service;
- enregistrement des événements relatifs à la sécurité;
- vérification automatique des services relatifs à la sécurité;
- établissement d'un chemin de confiance pour l'identification et la vérification de l'identité du personnel du service de certification;

- présence de processus de reprise pour les clés et l'application du service de certification;
- assurance de la robustesse des mécanismes empêchant qu'un processus informatique critique à la sécurité puisse être affecté ou corrompu par un autre processus informatique.

Le poste d'initialisation du service de certification doit être conforme aux exigences suivantes:

- contrôle de l'accès aux services de l'application de l'abonné;
- identification et vérification de l'identité des abonnés;
- protection contre la réutilisation des objets pour la mémoire vive et le disque rigide du poste;
- utilisation du chiffrement pour les sessions de communication et la sécurité des données sensibles;
- établissement d'un chemin de confiance pour l'identification et la vérification de l'identité du personnel du service de certification, de l'abonné ou d'un responsable d'un abonné qui n'est pas un individu;
- assurance de la robustesse des mécanismes empêchant qu'un processus informatique critique à la sécurité puisse être affecté ou corrompu par un autre processus informatique;
- système d'exploitation et application installés pour ne permettre que les protocoles et les commandes requises pour les services.

4.6.6 Contrôle de l'évolution du service de certification

4.6.6.1 Mesures de contrôle du développement des systèmes

Le développement et la conception des systèmes du service de certification doivent être faits par une firme certifiée ISO utilisant la méthodologie de conception « orientée objet ». Cette méthode doit utiliser :

- un système d'ingénierie automatisée assisté par ordinateur ou des outils de gestion appropriés;
- un système de vérification de l'application permettant de garantir qu'elle est conforme aux besoins du service de certification;
- un système de vérification des engagements contractés par le service de certification avec des tiers;
- un système encadrant l'acceptation de l'application;
- un système continu d'évaluation des risques;
- un système de mise à jour des mécanismes de sécurité.

4.6.6.2 Niveau d'évaluation de l'évolution du service de certification

L'application du service de certification doit être protégée par un sceau d'intégrité déterminé à partir du code exécutable apposé par l'organisation qui a la copie maîtresse. La valeur du sceau doit être fournie au service de certification par un support différent de l'application.

Au moment de l'installation, la valeur du sceau doit être recalculée à partir du code exécutable et confrontée à la valeur du sceau reçue. Le logiciel doit être installé uniquement si la bonne valeur est obtenue.

À chaque fois que l'application est lancée, ainsi que de façon périodique durant l'exécution, la valeur du sceau doit être recalculée à partir du code exécutable pour détecter s'il y a eu

modification de l'application. S'il y a eu modification du code exécutable, l'application du service de certification doit être arrêtée immédiatement et l'opérateur du poste de travail doit en être informé. Cette procédure doit être effectuée au minimum à toutes les 24 heures.

Les contrôles imposés sur le poste d'initialisation doivent rencontrer les exigences imposées sur le serveur du service de certification. Il n'y a pas de contrôle imposé sur les postes de travail utilisés par des AVI qui vérifient et font suivre l'information.

5. Format et contenu des certificats, du répertoire et des LCA

5.1 Des certificats

Cette section contient les règles et directives relatives à l'utilisation de certains types de certificats X.509.

Les types de certificats qui doivent être utilisés pour répondre aux exigences de l'Officier sont :

- les certificats de signature (notamment les certificats contenant le sceau du service de certification);
- les certificats de confidentialité (notamment les certificats de chiffrement de session);
- les certificats contenant les LCA.

Un certificat doit au moins comprendre les renseignements suivants :

- le nom distinctif du service de certification qui a délivré le certificat ainsi que sa signature (sceau);
- l'identifiant d'objet faisant référence aux présentes politiques et indiquant le type de certificat;
- la version de certificat et le numéro de série du certificat;
- le début et la fin de la période de validité du certificat;
- le nom distinctif de l'abonné.

L'inscription de renseignements aux certificats doit être effectuée, selon les circonstances, par les personnes et selon les procédures prévues dans les présentes politiques pour la délivrance, la rectification et la récupération de certificats. Seul l'abonné ou le responsable d'un abonné qui n'est pas un individu peut demander au service de certification l'inscription d'un renseignement aux certificats.

Les champs décrits dans cette section sont ceux qui, selon les exigences de l'Officier, doivent être complétés. Ces champs peuvent appartenir à un ou plusieurs types de certificats, lesquels sont décrits dans la norme X.509.

5.1.1 Champ « version »

Le service de certification doit inscrire dans ce champ le numéro de version de la norme X.509 utilisée soit 2 et plus pour les certificats contenant les LCA et 3 et plus pour les autres types de certificats.

5.1.2 Champ « numéro de série »

Le service de certification doit inscrire dans ce champ un numéro de série unique pour chaque certificat qu'il émet.

5.1.3 Champ « émetteur »

Le service de certification doit inscrire dans ce champ son nom distinctif.

5.1.4 Champ « validité »

Le service de certification doit inscrire dans ce champ la date et l'heure d'activation ainsi que la date et l'heure d'expiration du certificat.

5.1.5 Champ « sujet »

Le service de certification doit inscrire dans ce champ le nom distinctif de l'abonné.

5.1.6 Champ d'extension « type d'utilisation de la clé »

Le champ d'extension «type d'utilisation de la clé » indique si la clé inscrite dans le certificat doit servir à la validation de la signature ou si elle doit servir au chiffrement des envois.

5.1.7 Champ d'extension « numéro des politiques »

Le service de certification doit inscrire dans ce champ l' un des identifiants d'objets des présentes politiques.

5.1.8 Champ d'extension « équivalence entre les numéros de politiques »

Après une entente de reconnaissance autorisée par l'Officier, l'équivalence entre les présentes politiques et une politique utilisée par un autre service de certification devra être inscrite dans ce champ. Le cas échéant, le service de certification qui délivre un certificat doit inscrire dans ce champ les paires d'identifiants d'objet de politiques équivalentes ayant fait l'objet d'une entente de reconnaissance.

5.1.9 Champ d'extension « type de vérification des politiques »

Le service de certification doit compléter ce champ pour préciser que l'inscription du numéro de politiques est obligatoire dans le champ «numéro de politiques ». De plus, la présence de ce numéro doit être vérifiée par l'utilisateur avant de se fier au certificat.

5.1.10 Champ « code de raison »

Le service de certification doit inscrire dans ce champ la valeur « non spécifiée ».

5.1.11 Champs d'extension des LCA

Le service de certification doit supporter des sous-ensembles d'extensions normalisées.

5.1.12 Archivage des certificats d'un abonné

Aucun certificat délivré en vertu des présentes politiques n'est archivé. Le service de certification n'a pas à mettre en place de mesures permettant aux utilisateurs de déterminer, au moment d'une communication, si un certificat est archivé.

5.2 Du répertoire

Le répertoire doit être conforme à la norme X.500 et supporter le protocole LDAP version 2 ou 3.

Le répertoire contient les certificats de chiffrement des abonnés et les LCA. Aucune personne autre que le service de certification ne peut inscrire ou faire inscrire des renseignements au répertoire. Cependant, l'abonné peut demander au service de certification la rectification ou la suppression d'un renseignement le concernant. Sauf exception, le répertoire doit être accessible aux utilisateurs.

5.3 De la LCA

La LCA doit contenir les renseignements suivants :

- le nom distinctif du service de certification qui l'a délivrée;
- la date et l'heure de délivrance de la LCA;
- la date et l'heure de délivrance de la prochaine LCA;
- le numéro de série des certificats annulés (retirés, révoqués) et supprimés;
- le sceau du service de certification.

Dans tous les cas, la LCA ne doit comporter aucune information relative aux abonnés. Elle ne doit pas permettre de connaître le motif de l'annulation des certificats.

5.4 Périodicité et mise à jour des certificats, du répertoire et de la LCA

Toutes opérations subséquentes sur les certificats déclenchent, s'il y a lieu, la mise à jour des certificats et du contenu du répertoire.

La LCA doit être mise à jour et diffusée au minimum à toutes les 12 heures. De plus, elle est mise à jour immédiatement à la suite de l'annulation d'un certificat.

5.5 Renseignements dont l'exactitude est confirmée

Le service de certification confirme l'exactitude de l'information dont l'inscription au certificat est obligatoire selon la section 5.1 des présentes politiques.

Toutefois, le service de certification ne confirme aucunement l'exactitude de tout autre renseignement inscrit au certificat.

Le service de certification confirme l'exactitude de la LCA inscrite au répertoire.

5.6 Limite à l'utilisation des certificats et du répertoire

Les clés et les certificats délivrés dans le cadre des présentes politiques ne peuvent être utilisés que dans le cadre de transactions, d'applications ou d'échanges électroniques avec le Bureau de la publicité des droits personnels et réels mobiliers.

La clé privée du service de certification doit être utilisée pour apposer le sceau d'intégrité sur les certificats et la LCA.

Les présentes politiques n'imposent aucune limite relativement à la valeur des transactions dans le cadre desquelles les clés et les certificats peuvent être utilisés.

6. Administration des politiques

6.1 Procédures de modification

6.1.1 Avis de modification

Le responsable des politiques doit aviser les abonnés et les utilisateurs de tout changement des présentes politiques qui, selon son évaluation, a un impact sur un nombre important d'abonnés ou d'utilisateurs.

6.1.2 Forme de diffusion des avis

Dans les cas nécessitant un avis, le responsable doit informer les abonnés, les utilisateurs et les autres services de certification ayant conclu une entente de reconnaissance dans le cadre des présentes politiques des modifications à celles-ci. L'avis peut être transmis par courrier électronique ou publié sur le site Internet du RDPRM.

6.1.3 Éléments qui requièrent de nouvelles politiques

Si des changements de politiques ont, selon l'évaluation du responsable des politiques, un impact majeur sur la majorité des abonnés ou des utilisateurs, ce responsable peut, à sa discrétion, produire de nouvelles politiques avec un nouvel identifiant d'objet.

6.2 Procédure de diffusion

6.2.1 Diffusion des politiques

Les présentes politiques doivent être accessibles aux utilisateurs. Elles peuvent être accessibles sur le site Internet du RDPRM. Le service de certification doit également les rendre accessibles.

L'Officier publie sur le site Internet du RDPRM toute autre information additionnelle qui doit être portée à la connaissance des abonnés et utilisateurs, notamment en ce qui a trait à la mise à jour des limites à l'utilisation des clés et certificats, le cas échéant.

6.2.2 Pratiques de certification

Les pratiques de certification du service de certification ne sont pas diffusées. Elles sont toutefois mises à la disposition de l'Officier et du vérificateur.

6.2.3 Contrôle de l'accès

Si les présentes politiques sont diffusées sur un site Internet, des contrôles doivent être mis en place pour sécuriser la création et la modification de tels documents.

6.3 Vérification de la conformité

6.3.1 Vérification de la conformité du service de certification

Le service de certification reconnu par le responsable des présentes politiques doit se soumettre aux normes de vérification établies par le ministère de la Justice du Québec ou par le Gouvernement du Québec. Une vérification de la conformité doit être faite à leur demande suivant un préavis de trois mois.

Cette vérification doit comprendre une comparaison entre les pratiques du service de certification et les présentes politiques. Ainsi, à chaque vérification de la conformité, le vérificateur s'assure que le service de certification respecte les exigences des présentes politiques.

Les résultats de la vérification seront communiqués au service de certification qui doit prendre les mesures nécessaires pour corriger les éléments non conformes. Le service de certification communique les résultats au responsable des présentes politiques et, s'il y a lieu, à tout autre service de certification ayant conclu une entente de reconnaissance avec le service de certification vérifié. Toutefois, dans un souci de protection des renseignements personnels et du maintien de la sécurité du service, le service de certification peut rendre certains éléments de la vérification non disponibles tels que l'information sur le personnel, les caractéristiques de sécurité du réseau, le contenu de la correspondance et l'information de sauvegarde.

Pour effectuer une vérification de conformité des opérations du service de certification, le vérificateur doit posséder une expérience pertinente dans le domaine de la vérification. Le vérificateur et l'entité vérifiée ne doivent avoir aucune relation financière, légale ou autre pouvant constituer un conflit d'intérêts.

6.3.2 Vérification de la conformité de l'AVI

La vérification du respect des obligations imposées à l'AVI est assurée par la validation des comptes rendus transmis au service de certification et par les contrôles faits dans le cadre de l'inspection professionnelle par l'Ordre auquel appartient l'AVI.

À défaut de conformité, le service de certification peut prendre toute mesure qui lui semble appropriée. De plus, l'Officier peut retirer à l'AVI l'autorisation d'agir à ce titre.

6.3.3 Vérification de la conformité des utilisateurs

Les utilisateurs ne sont pas sujets à une procédure de vérification de la conformité, à l'exception du service de certification.

7. Dispositions diverses

7.1 Protection des renseignements personnels

Tous les renseignements recueillis, utilisés, conservés ou communiqués par le service de certification ou par les AVI sont assujettis, selon le cas, à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) ou à la *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q, c. P-39.1).

Notamment, toutes les informations recueillies dans le cadre de la délivrance ou de la gestion des clés et des certificats ne doivent être utilisées ou communiquées que pour les fins pour lesquelles elles ont été recueillies.

7.2 Mécanismes de traitement des plaintes

Tout abonné ou tout utilisateur peut déposer une plainte concernant le service de certification ou concernant un AVI en s'adressant au responsable du service de certification.

Lorsque le service de certification est dans l'impossibilité de traiter la plainte à la satisfaction de cet abonné ou de cet utilisateur, il doit la transmettre au responsable des présentes politiques.

7.3 Garanties et limites à la responsabilité

Le service de certification garantit qu'il a pris les moyens raisonnables pour s'assurer que les renseignements dont il confirme l'exactitude en vertu de la section 5.5 sont exacts. Toutefois, cette garantie ne s'étend pas à l'exactitude de tout autre renseignement pouvant être inscrit dans un certificat ou dans un répertoire.

Le service de certification décline également toute responsabilité à l'égard des certificats portant la mention «certificat d'essai » ou toute autre mention de même nature indiquant qu'on ne peut raisonnablement s'y fier.

Aucune responsabilité ne sera assumée par le service de certification ou par son personnel pour l'utilisation par un abonné ou un utilisateur d'un certificat de manière non conforme par les présentes politiques.

Nul ne saurait être tenu responsable pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant des présentes politiques lorsque les circonstances y donnant lieu relèvent de la force majeure au sens de l'article 1470 du *Code civil du Québec* ou d'un cas fortuit.

7.4 Tarifs

Le service de certification peut imposer aux utilisateurs un tarif pour les services qu'il rend en vertu des présentes politiques.

7.5 Interprétation et mise en application

7.5.1 Lois et règlements applicables

Les présentes politiques sont régies et interprétées conformément aux lois et règlements applicables au Québec, bien que les activités qui découlent des présentes politiques soient exécutées en partie hors du Québec.

7.5.2 Règlement des différends

En cas de contestation, les parties font attribution de juridiction aux tribunaux compétents de la province de Québec. Conformément à l'article 3.1.2.4 des présentes, le service de certification a la compétence exclusive en matière d'attribution des noms distinctifs.

7.5.3 Indépendance des dispositions

Le fait pour une ou plusieurs dispositions des présentes politiques d'être déclarées invalides, illégales ou inapplicables ne portent pas atteinte à la validité des autres dispositions.