Agence des douanes et du revenu du Canada
Canada Customs and Revenue Agency

Confidentialité

Politique de certification d'assurance de niveau moyen

pour

l'Agence des douanes et du revenu du Canada

Autorité de certification externe

Version 1.3b

décembre 2002

CONTRÔLE DES DOCUMENTS

Version	Date	Auteur	Motif
1.3a	**Mai 2001**	**B. Lusk**	**Mise en forme et changements grammaticaux mineurs**
1.3b	**déc. 2002**	**B. Robin**	**Mise-à-jour de l'information personne-ressource**

Table des matières

1. Introduction

1.1 Aperçu

La politique de certification définie dans le présent document s'adresse à l'Agence des douanes et du revenu du Canada (ADRC). Les utilisateurs du présent document doivent consulter l'autorité de certification de délivrance afin d'obtenir de plus amples détails sur la mise en place de la présente politique de certification.

La politique PolcertconfidICP a trait à la gestion et à l'emploi de certificats renfermant des clés publiques utilisées pour l'établissement de clés, y compris le transfert de clés. Les certificats délivrés dans le cadre de la présente politique visent à assurer la confidentialité des applications, notamment de courrier électronique, ou des communications sur le Web, en plus de la protection des renseignements désignés par la Politique gouvernementale en matière de sécurité (PGS). Ils ne visent pas à assurer la protection des renseignements classifiés.

Le terme «assurance» ne vise pas à émettre la représentation ou la garantie que les services d'AC sont disponibles à 100 p. cent dans le cadre de l'ICP d'ADRC. Une telle disponibilité peut être affectée par la maintenance du système, par la réparation du système ou par des facteurs hors du contrôle de l'AC.

La délivrance d'un certificat de clés publiques dans le cadre de la présente politique ne suppose pas que l'abonné ait le pouvoir d'effectuer des transactions commerciales au nom de l'Agence des douanes et du revenu du Canada exploitant l'AC.

L'AC sera régie par les lois du Canada et par les lois provinciales pertinentes concernant la mise en exécution, la construction, l'interprétation et la validité de la présente politique de certification.

L'Agence des douanes et du revenu du Canada se réserve le droit de ne pas passer d'entente de cocertification avec une autorité de certification externe.

1.1.1 Aperçu de la politique

La présente politique porte la désignation d'identificateur d'objet suivante : 2 16 124 101 1 272 3 1 1 0 2.

La présente politique a été conçue aux fins d'emploi dans certaines situations et désigne les responsabilités et rôles précis de l'AC qui émet les certificats et des autorités locales d'enregistrement qui doivent accomplir les tâches pouvant leur être attribuées par l'AC. Les abonnés et les parties utilisatrices ont également des obligations précises dont les grandes lignes sont décrites dans la présente politique.

L'AC peut délivrer des cocertificats à ce niveau d'assurance.

L'AC doit s'assurer qu'elle s'associe à un certificat et à un dépôt de Listes de certificats révoqués (LCR) pour ce type de certificat et qu'elle utilise ceux-ci. Les certificats doivent être mis à la disposition des abonnés.

L'emploi des clés de confidentialité d'assurance de niveau moyen est approprié à la confidentialité des renseignements désignés dont l'atteinte à l'intégrité pourrait entraîner un préjudice grave dans le cas d'un intérêt non national.

La Couronne aux droits du Canada et l'ADRC déclinent toute responsabilité quant à l'emploi de ce type de certificat pour d'autres usages que ceux permis par l'AC. La Couronne aux droits du Canada et l'ADRC limitent leur responsabilité aux emplois permis à 50 000 $ par cas d'emploi.

Tout différend relatif à la gestion des clés ou des certificats dans le cadre de la présente politique doit être réglé par les parties concernées à l'aide du mécanisme de règlement des différends contenu dans le présent document.

Des certificats peuvent être délivrés dans le cadre de la présente politique par suite de l'authentification de l'identité d'un abonné. L'identification sera accomplie suivant la manière décrite dans la présente politique.
L'AC révoquera les certificats suivant les circonstances énumérées dans la présente politique.

L'AC doit conserver des dossiers ou des journaux de renseignements de la manière décrite dans la présente politique.

L'AC devrait s'assurer que les fonctions critiques de l'AC sont accomplies par au moins deux personnes.

Les clés peuvent comporter une période de validité comme l'indique la présente politique. Les clés de confidentialité délivrées par l'AC seront sauvegardées afin d'empêcher la perte ou la corruption des données.

Aucun renseignement personnel recueilli par l'AC peut être divulgué sans le consentement de l'abonné, à moins que la loi ne l'exige.

Les activités de l'AC sont soumises à une inspection.

1.1.2 Définitions générales

Abonné	Personne ou organisme dont la clé publique est certifiée dans un certificat à clé publique. Dans le contexte de l'ICP d'ADRC, un abonné peut être un fonctionnaire ou un citoyen ou encore un client ou un fournisseur du gouvernement. Les abonnés peuvent détenir un ou plusieurs certificats de la part d'une AC précise qui leur est associée; la plupart auront au moins deux certificats actifs - l'un contenant leur clé de vérification de signature numérique; l'autre renfermant leur clé de chiffrement de confidentialité.
AC de délivrance	Dans le contexte d'un certificat particulier, l'AC de délivrance est l'AC qui a signé et délivré le certificat.
Arborescence des renseignements de répertoire (ARR)	Structure hiérarchique logique des renseignements de répertoire.
Autorité d'accréditation	Entité de gestion de l'ICP (EGI) ayant le pouvoir de permettre à une entité d'ICP subalterne d'exploiter un domaine particulier. L'EGI constitue l'autorité d'accréditation pour toutes les connexions à l'ICP d'ADRC. Une unité ou une section particulière d'un ministère peut jouer le rôle d'autorité d'accréditation pour l'AC.
Autorité de certification (AC)	Autorité en qui un ou plusieurs utilisateurs mettent leur confiance pour délivrer et gére les LCR et certificats à clé publique conformes X.509. Chaque AC dans une ICP du G peut délivrer des certificats selon un choix de politiques d'après le niveau d'assurance pour lequel l'AC a été accréditée ainsi que d'après les exigences et le rôle de l'abonné
Autorité de gestion des politiques (AGP)	Entités du GC et d'ADRC responsables de l'établissement, de la mise en place et de l'administration des décisions politiques relatives aux PC et aux ÉPC par l'entremise des ICP du GC et d'ADRC.
Autorité fonctionnelle	Personnel ministériel responsable du fonctionnement global de l'AC de l'ICP d'ADRC.
Autorité locale d'enregistrement (ALE)	Personne ou organisme responsable de l'identification et de l'authentification des abonnés de certificats avant la délivrance des certificats, mais qui ne signe ni n'émet dans les faits ceux-ci. Une ALE reçoit certaines tâches au nom de l'AC.
Certificat	Clé publique d'un utilisateur, accompagnée des renseignements connexes, signée de façon numérique avec la clé privée de l'autorité de certification qui l'a délivrée. Le format du certificat est conforme à la Recommandation UIT-T X.509.
Cocertificat	Certificat servant à établir un lien de confiance entre deux autorités de certification.
Dépôt	Répertoire de stockage des LCR, des LCAR et des certificats aux fins d'accès par les entités finales.
Données d'activation	Données privées (autres que des clés) qui sont nécessaires à l'accès des modules de chiffrement.
Employé	Personne employée par un «ministère», terme défini ci-dessus.
Énoncé de pratiques de certification (ÉPC)	Énoncé des pratiques qu'une autorité de certification emploie aux fins de délivrance d certificats. L'ÉPC décrit l'équipement, les politiques et les procédures mis en place pa l'AC afin de satisfaire aux spécifications énoncées dans les politiques de certification appuyées par l'AC.

Entité	Tout élément autonome dans l'Infrastructure à clé publique. Il peut s'agir d'une AC, d'une ALE ou d'une entité finale.
Entité finale	Entité utilisant les clés et certificats créés dans l'ICP pour des fins différentes de celles de la gestion des clés et certificats susmentionnés. Une entité finale peut être un abonné, une partie utilisatrice, un dispositif ou une application.
Identificateur d'objet (IDO)	Identificateur alphanumérique/numérique enregistré dans le cadre de la norme d'enregistrement ISO pour faire référence à un objet ou à une catégorie d'objet précis Dans l'ICP d'ADRC, cet identificateur sert à désigner de façon unique chacune des politiques et algorithmes de chiffrement soutenus.
Infrastructure à clé publique (ICP)	Ensemble des politiques, processus, environnements serveurs, logiciels et postes de travail servant à l'administration des certificats et des clés.
Installation centrale canadienne (IC	Autorité de certification centrale de l'ICP du gouvernement du Canada. Sous la direction de l'AGP du GC, l'ICC signe et gère les cocertificats des AC de haut niveau des ministères du GC. L'ICC signe et gère également les cocertificats avec les AC autres que celles du GC. L'ICC ne gère pas les certificats des abonnés.
Intégrité des données	Assurance que les données demeurent inchangées entre le moment de leur création le moment de leur réception.
Liste des certificats de l'autorité révoqués (LCAR)	Liste des certificats de l'autorité révoqués. Une LCAR constitue une LCR pour les cocertificats.
Liste des certificats révoqués (LCR)	Liste conservée par une autorité de certification pour les certificats qu'elle a délivrés e qui sont révoqués avant leur expiration naturelle.
Logiciel d'autorité de certification	Logiciel de chiffrement nécessaire à la gestion des clés des entités finales.
MD5	Un des algorithmes de compilation de messages élaboré par RSA Data Security Inc.
Ministère	Toute entité définie à l'Annexe 1, Parties I et II de la Loi sur les relations de travail dar la fonction publique; les Forces canadiennes et la Gendarmerie royale du Canada.
Nom distinctif (ND)	Nom complet d'une entrée de répertoire. Le nom distinctif se compose du nom distinc relatif (NDR) et des NDR de chaque entrée reliant directement l'entrée et la racine de l'arborescence.
Nom distinctif relatif (NDR)	Ensemble de types d'attributs et de valeurs distinctives qui désignent de façon unique une entrée parmi ses semblables dans l'ARR. Ces attributs peuvent comprendre un nom commun, un organisme et un pays.
Organisme	Ministère, organisme, société, partenariat, fiducie, coentreprise ou toute autre association ou tout autre organisme d'état.
Parrain	Dans l'ICP d'ADRC, direction, entité d'ADRC ou fonctionnaire qui a déterminé qu'un certificat devrait être délivré à une personne ou à un organisme. Dans le cas d'un certificat pour un citoyen ou une entreprise commerciale, le parrain pourrait être le gestionnaire de l'unité d'affaires d'ADRC qui comporte l'exigence de communiquer av cette entité. Le parrain pourrait suggérer un ND approprié pour le certificat et sera responsable de fournir ou de confirmer les détails des attributs des certificats à l'ALE. Le parrain est également responsable d'informer l'AC ou l'ALE si le rapport du ministè avec l'abonné a pris fin ou a changé de telle sorte que le certificat devrait être révoqu ou mis à jour.
Partie utilisatrice	Personne qui utilise un certificat signé par l'ACP de l'ICP d'ADRC afin d'authentifier u signature numérique ou de chiffrer les communications au sujet du certificat et constitue un abonné de l'AC de l'ICP d'ADRC ou une ICP qui est cocertifiée avec l'IC d'ADRC.
Politique de certification (PC)	Ensemble identifié de règles indiquant l'applicabilité d'un certificat à une collectivité donnée ou à une catégorie d'applications comportant des exigences de sécurité communes. Par exemple, une politique de certification particulière pourrait indiquer l'applicabilité d'un type de certificat à l'authentification de transactions d'échange de données informatisé pour le commerce de biens dans une plage de prix donnée.
Signature numérique	Résultat de la transformation d'un message à l'aide d'un système de chiffrement utilisant des clés de manière à ce que la personne qui reçoit le message initial puisse déterminer : (a) si la clé qui a servi au codage est bien celle du signataire; et (b) si le message a été modifié depuis le moment de son codage.

1.1.3 Définitions de la politique sur la sécurité du gouvernement

Classifié	Tout renseignement dont on peut croire que toute atteinte à son intégrité pourrait porter préjudice à l'intérêt national. Les renseignements de ce type portent

	habituellement la mention CONFIDENTIEL, SECRET ou TRÈS SECRET selon la gravité du préjudice.
De nature extrêmement délicate	A trait à la quantité très limitée de renseignements dont l'atteinte à l'intégrité pourra raisonnablement entraîner un préjudice extrêmement grave dans le cas d'un intérêt non national, par exemple, la mort. Les renseignements de ce type peuvent porter mention ***PROTÉGÉ C***.
De nature particulièrement délicate	A trait à des renseignements dont l'atteinte à l'intégrité pourrait entraîner un préjudice grave dans le cas d'un intérêt non national, par exemple, la perte de réputation ou un avantage concurrentiel. Les renseignements de ce type peuvent porter la mention ***PROTÉGÉ B***.
De nature peu délicate	A trait à des renseignements dont l'atteinte à l'intégrité pourrait raisonnablement entraîner un préjudice dans le cas d'un intérêt non national, par exemple, la divulgation d'une somme salariale exacte. Les renseignements de ce type peuvent porter la mention ***PROTÉGÉ A*.**
Vérification approfondie de la fiabilité (VAF)	Évaluation de l'intégrité d'une personne; condition pour obtenir la cote de fiabilité approfondie.
Zone d'accès public	Entoure habituellement une installation du gouvernement ou en fait habituellement partie. Les terrains environnant un édifice ainsi que les corridors publics et les foyer d'accès aux ascenseurs dans des édifices à locataires multiples constituent des exemples. Les désignatifs de limites comme les signes et la surveillance directe ou distante peuvent servir à décourager toute activité non autorisée.
Zone de réception	Entrée d'une installation où survient le contact initial entre le public et le ministère, où sont fournis les services, où sont échangés les renseignements et où est limité l'accès aux zones limitées (zones d'opérations, zones sécuritaires et zones hautement sécuritaires). L'activité dans une zone de réception est surveillée à divers degrés par le personnel qui y travaille, par d'autres membres du personnel ou par du personnel de sécurité. L'accès au public est limité à des heures précises de la journée ou pour des raisons précises. L'entrée au-delà de la zone de réception est indiquée par un périmètre reconnaissable comme des portes ou une disposition de meubles et de divisions dans un environnement de bureau éclaté.
Zone de sécurité	Secteur dans lequel l'accès est limité au personnel autorisé et aux visiteurs autorisés et escortés de façon appropriée. Les zones de sécurité devraient être accessibles de préférence depuis une zone d'opérations et depuis un point d'entrée précis. Il n'est pas nécessaire qu'une zone de sécurité soit séparée d'une zone d'opérations par un périmètre de sécurité. Une zone de sécurité devrait être surveillée 24 heures par jour, 7 jours sur 7, par du personnel de sécurité, par d'autres membres du personnel ou par des moyens électroniques.
Zone d'opérations	Zone où l'accès est limité au personnel qui y travaille et aux visiteurs escortés de façon appropriée. Les zones d'opérations devraient être surveillées au moins de façon périodique, d'après une évaluation de la menace et des risques (EMR) et devraient être accessibles de préférence depuis une zone de réception.
Zone hautement sécuritaire	Zone dans laquelle l'accès est contrôlé par un point d'entrée et est limité au personnel autorisé ayant été soumis à une enquête de sécurité appropriée et aux visiteurs escortés de façon appropriée. Les zones hautement sécuritaires ne devraient être accessibles que depuis les zones sécuritaires et sont séparées des zones sécuritaires et des zones d'opérations par un périmètre construit selon les spécifications recommandées par l'ÉMR. Les zones hautement sécuritaires sont surveillées 24 heures par jour, 7 jours sur 7, par du personnel de sécurité, par d'autres membres du personnel ou par des moyens électroniques.

1.1.4 Acronymes

AC	Autorité de certification
ADC	Appel de commentaires
ADRC	Agence des douanes et du revenu du Canada
AGP	Autorité de gestion des politiques
ALE	Autorité locale d'enregistrement
ARR	Arborescence des renseignements de répertoire
CST	Centre de la sécurité des télécommunications
ÉMR	Évaluation de la menace et des risques
ÉPC	Énoncé de pratiques de certification
GC	Gouvernement du Canada

ICC	Installation centrale canadienne
ICP	Infrastructure à clé publique
ICPX	Infrastructure à clé publique X.509
IDO	Identificateur d'objet
IETF	Groupe Internet Engineering Task Force
LCAR	Liste des certificats de l'autorité révoqués
LCR	Liste des certificats révoqués
ND	Nom distinctif
NDR	Nom distinctif relatif
NIP	Numéro d'identification personnelle
NIST	National Institute of Standards and Technology
PC	Politique de certification
PSG	Politique sur la sécurité du gouvernement, Gouvernement du Canada
PUB FIPS	Publication Federal Information Processing Standard (Etats-Unis)
RSA	Rivest-Shamir-Adleman
SHA-1	Algorithme de chiffrement irréversible
UIT	Union internationale des télécommunications
URL	Localisateur de ressources universel
VAF	Vérification approfondie de la fiabilité

1.2 IDO alphanumérique d'identification

La présente politique de certification porte le nom suivant : ADRC External Medium Assurance Confidentiality PC – PC d'ADRC relative à la confidentialité externe d'assurance de niveau moyen.

La présente politique porte la désignation d'identificateur d'objet (IDO) suivante : 2 16 124 101 1 272 3 1 1 0 2.

1.3 Clientèle et applicabilité

La présente politique de certification a été conçue pour satisfaire les exigences de certification du grand public en matière de clés d'ADRC.

1.3.1 Autorités de certification (AC)

L'AC régie par la présente politique est responsable des aspects suivants :

- création des paires de clés de confidentialité des entités finales;
- création et signature des certificats liant les abonnés et le personnel de l'ICP avec leurs clés de chiffrement publiques;
- promulgation de l'état des certificats par l'entremise des LCR; et
- assurance du respect de la politique de certification.

Bien qu'ADRC puisse faire appel à un entrepreneur pour fournir les services d'AC, cet organisme doit demeurer responsable et comptable de l'exploitation de son AC.

L'AC d'ADRC effectuera une cocertification par l'entremise de l'ICC. Une cocertification doit être conforme à la politique de certification et à toute exigence supplémentaire déterminée par ADRC et par les AGP du GC. Toute cocertification entre les AC des ICP d'ADRC et les AC ne faisant pas partie d'ADRC sera accomplie par l'entremise de l'ICC conformément aux instructions de l'AGP du GC. Toute entente intervenue avec d'autres AC doit être documentée. Les dénis de responsabilités pertinents doivent être mis à la disposition des abonnés.

Nonobstant les points susmentionnés, l'AC peut délivrer des cocertificats à d'autres AC où l'AGP du GC l'autorise expressément.

1.3.2 Autorités locales d'enregistrement (ALE)

Une ALE régie par la présente politique de certification est responsable de toutes les tâches qui lui sont attribuées par l'AC.

Une ALE peut accomplir des tâches au nom de plusieurs AC, pourvu qu'elle satisfait toutes les exigences de la présente PC dans l'exécution de ces tâches.

1.3.3 Dépôts

L'AC doit s'assurer qu'il existe au moins un certificat et un dépôt des LCR connexe. Ce dépôt devrait se présenter sous la forme d'un ou de plusieurs répertoires conformes au profil des normes X.550 du GC.

Un dépôt peut être ou non sous le contrôle de l'AC. Si un dépôt n'est pas sous le contrôle de l'AC, cette dernière doit s'assurer que les conditions de son association comprennent sans s'y limiter les sujets de disponibilité, de contrôle d'accès, d'intégrité des données ainsi que de reproduction et d'enchaînement de répertoires.

1.3.4 Abonnés

Les personnes ou organismes peuvent être des abonnés. Ces derniers peuvent se voir délivrer des certificats aux fins d'attribution de dispositifs, de rôles organisationnels ou d'applications, pourvu que la responsabilité et la comptabilité soit attribuables à une personne ou à un organisme.

Les certificats d'ICP d'ADRC ne seront délivrés qu'après dépôt d'une demande ou qu'après autorisation de délivrance de la part d'un ou de plusieurs parrains. Ils peuvent être délivrés à des personnes, à des organismes ou à d'autres entités avec qui le parrain entretient un rapport.

L'admissibilité à un certificat est laissée à la seule discrétion de l'AC.

L'AC peut administrer tout nombre d'abonnés.

1.3.5 Parties utilisatrices

Une partie utilisatrice peut être soit un abonné de l'ICP d'ADRC, soit un abonné d'une ICP qui a signé une entente de cocertification avec l'ICP d'ADRC.

1.3.6 Applicabilité de la politique

La présente politique est souhaitable pour les emplois des certificats tels que l'établissement des clés de confidentialité des renseignements qui, s'ils étaient altérés, il est raisonnable de penser, causeraient un préjudice sérieux ne revêtant toutefois pas un intérêt national. La Politique gouvernementale en matière de sécurité désigne ce type de renseignements comme **PROTÉGÉ B**.

1.3.6.1 Applications approuvées et interdites

L'AC doit certifier quelles applications d'ADRC doivent servir avec le système d'ICP. Ces dernières doivent au minimum satisfaire les exigences suivantes :

- établir, transférer et exploiter de façon appropriée les clés publiques et privées;
- pouvoir effectuer la validité et la vérification des certificats de façon appropriée; et
- faire état des renseignements et des avertissements appropriés à l'abonné.

1.4 Détails sur les contacts

La présente politique est administrée par :

Direction générale de l'informatique
Direction de l'intégration des services et de l'architecture
Section de l'infrastructure à clé publique
25 Fitzgerald, C4-130
Ottawa (Ontario) Canada
K1A 0L5

La personne-ressource est :

Adresse de courriel : **Sylvain.Tremblay@ccra-adrc.gc.ca**

Téléphone : (613) 948-0813, Télécopieur : (613) 948-1002

2. Dispositions générales

2.1 Obligations

2.1.1 Obligations de l'AC

L'AC travaillera conformément à l'ÉPC, la présente PC et les lois du Canada pour la délivrance et la gestion des clés fournies aux ALE et aux abonnés dans le cadre de la présente PC. L'AC s'assurera que toutes les ALE travaillant en son nom se conformeront aux dispositions pertinentes de la présente PC régissant le travail des ALE. L'AC prendra toutes les mesures raisonnables pour s'assurer que les abonnés et les parties utilisatrices soient conscients de leurs obligations et droits respectifs en ce qui a trait à l'exploitation et à la gestion de clés, de certificats ou de matériel et de logiciels d'entités finales utilisés avec l'ICP.

L'AC doit fournir un avis relatif aux limitations de responsabilité. Un tel avis doit au moins être fourni avec le certificat par l'entremise d'une extension de certificats privés ou par l'emploi du champ **userNotice** dans le certificat, comme le définit l'ICPX. Étant donné les limites d'espace d'un certificat, un tel avis doit être limité au langage suivant «Limited Liability. See CP-Responsabilité limitée. Voir PC.”

- L’IDO pour **ccraCertUserNotice** est 2 16 124 101 1 272 3 0 0.

L'AC doit :

- délivrer un ÉPC;
- avoir en place des mécanismes et procédures afin de s'assurer que ses ALE et abonnés sont au courant des dispositions de la présente politique qui s'appliquent à eux et qu'ils consentent à les respecter;
- s'assurer que toute AC avec qui il effectue une cocertification directe se conforme à toutes les CP mutuellement reconnues; et
- démontrer, par inspection de conformité, aux AC de cocertification, qu'elle se conforme à la présente PC.

Le personnel de l'AC associé aux rôles de l'ICP doit être individuellement comptable des gestes qu'il pose. L'expression «individuellement comptable» signifie qu'une preuve doit démontrer qu'un geste est propre à la personne posant le geste.

2.1.1.1 Avis de délivrance et de révocation de certificats

L'AC de délivrance doit mettre les LCR à la disposition de l'abonné ou de la partie utilisatrice conformément à l'article 4.4. Elle doit aviser un abonné de la délivrance ou de la révocation d'un certificat portant le ND de l'abonné.

2.1.1.2 Exactitude des représentations

Quand l'AC de délivrance publie un certificat, elle certifie qu'elle a délivré un certificat à un abonné et que les renseignements qui y sont énoncés ont été vérifiés conformément à la présente PC. La publication du certificat dans un dépôt auquel a accès l'abonné constitue un avis d'une telle vérification.

L'AC fournira à chaque abonné un avis des droits et obligations de celui-ci dans le cadre de la présente politique de certification. Un tel avis peut se présenter sous forme d'un Énoncé des utilisations acceptables de l’ICP de l’ADRC. Un tel avis comprendra une description des usages permis des certificats délivrés dans le cadre de la présente; des obligations de l'abonné relativement à la protection des clés; et des procédures de communication entre l'abonné et l'AC ou l'ALE, y compris la communication de modifications concernant la prestation du service ou les modifications apportées à la présente politique. Les abonnés devraient également être avisés des procédures à suivre en cas d'atteinte à l'intégrité soupçonnée des clés, pour le renouvellement de certificats ou de clés, pour l'annulation du service et pour le règlement de différends.

L'AC s'assurera que tout avis relatif aux droits et obligations de l'abonné dans le cadre de la présente politique de certification comprend une description des obligations de la partie utilisatrice en ce qui concerne l'emploi, la vérification et la validation de certificats.

2.1.1.3 Temps écoulé entre la demande et la délivrance d'un certificat

Il n'existe aucune disposition relative à la période s'écoulant entre le moment de réception d'une demande de certificat et la production des effets de clés de l'entité.

L'AC doit s'assurer que les effets de clés de l'entité seront acheminés à celle-ci dans les 24 heures suivant leur production.

L'AC doit s'assurer que la période au cours de laquelle l'entité doit terminer son processus d'initialisation ne dépasse pas cinq jours à partir de la date de production des effets de clés de l'entité par l'AC.

2.1.1.4 Révocation et renouvellement de certificats

L'AC de délivrance doit s'assurer que toute procédure d'expiration, de révocation et de renouvellement d'un certificat sera conforme aux dispositions pertinentes de la présente PC et que ces procédures seront énoncées expressément dans l'entente avec l'abonné ainsi que dans tout autre document applicable décrivant les conditions d'emploi du certificat. L'AC doit s'assurer que les procédures de renouvellement de clés sont conformes à l'article 4.7. L'AC de délivrance doit également s'assurer qu'un avis de révocation d'un certificat sera affiché dans la LCR selon les délais énoncés aux alinéas 4.4.4 et 4.4.9. L'adresse de la LCR doit être définie dans le certificat.

2.1.1.5 Protection des clés privées

L'AC doit s'assurer que les clés privées qu'elle conserve ou enregistre ainsi que les données d'activation sont protégées conformément aux articles 5 et 6.

Toutes les autres entités doivent s'assurer que leurs clés privées et données d'activation sont protégées conformément aux articles 5 et 6.

L'AC de délivrance doit veiller à ce que toute clé privée de confidentialité d'un abonné qu'elle a sauvegardée ou archivée soit protégée conformément à l'article 6. Elle ne peut pas divulguer les clés privées de confidentialité à tout autre tiers sans le consentement préalable de l'abonné ou du promoteur, à moins que la loi l'exige.

2.1.1.6 Restrictions relatives à l'emploi des clés privées délivrées pour l'AC

L'AC doit s'assurer que sa clé privée de signature de certificats est utilisée uniquement pour la signature de certificats et de LCR.

L'AC doit s'assurer que les clés privées délivrées à son personnel aux fins d'accès et d'exploitation des applications de l'AC ne servent qu'à ces seules fins. Au besoin, le personnel se verrait délivrer des ensembles de clés et de certificats d'abonnés pour des fins autres que celles visées pour l'AC.

2.1.2 Obligations de l'ALE (tâches de l'ALE)

L'AC doit s'assurer que toutes ses ALE se conforment aux dispositions pertinentes de la présente PC et des ÉPC de l'AC.

L'AC est responsable, par l'entremise de son personnel d'ALE, d'informer abonnés de tous renseignements pertinents concernant les droits et obligations de l'AC, de l'ALE et de l'abonné présentés dans la présente PC, dans l'entente avec l'abonné, le cas échéant et dans tout autre document pertinent décrivant les conditions d'emploi.

Les dossiers de consignation des mesures entreprises au cours de l'accomplissement des tâches des ALE doivent désigner la personne ayant accompli la tâche particulière.

Les administrateurs des ALE doivent être individuellement comptables des gestes qu'ils posent au nom de l'AC. L'expression «individuellement comptable» signifie qu'une preuve doit démontrer qu'un geste est propre à la personne posant le geste.

2.1.2.1 Avis de délivrance et de révocation de certificats

Il n'existe aucune exigence mentionnant qu'une ALE doive aviser une partie utilisatrice de la délivrance ou de la révocation d'un certificat.

2.1.2.2 Exactitude des représentations

Quand une ALE soumet des renseignements sur l'abonné à l'AC, elle doit certifier à l'AC qu'elle a authentifié l'identité de cet abonnée conformément aux articles 3 et 4.

2.1.2.3 Protection des clés privées de l'ALE

Chaque personne accomplissant les tâches d'une ALE en ligne grâce à une application d'administration distante avec l'AC doit s'assurer que ses clés privées sont protégées conformément aux articles 5 et 6.

2.1.2.4 Restrictions relatives à l'emploi des clés privées délivrées pour l'ALE

Les clés privées utilisées par l'administrateur d'une ALE aux fins d'accès et d'exploitation des applications de l'ALE en ligne avec l'AC ne doivent pas servir à d'autres fins.

2.1.3 Obligations de l'abonné

L'AC de délivrance doit s'assurer qu'un abonné convienne d'une entente ou qu'il consente à respecter un Énoncé des utilisations acceptables de l'ICP de l'ADRC décrivant les conditions d'emploi, y compris les applications et fins permises.

2.1.3.1 Représentations

Tout renseignement devant être soumis à l'AC ou à l'ALE relativement à un certificat doit être complet et exact.

2.1.3.2 Protection des clés privés et des jetons de clés de l'abonné

Les abonnés doivent protéger leurs clés privées et les jetons de clés (le cas échéant) conformément à l'article 6 et ils doivent prendre toutes les mesures raisonnables afin d'empêcher la perte, la divulgation, la modification ou l'usage non autorisé des clés et des jetons.

2.1.3.3 Restrictions relatives à l'emploi des clés privées pour l'entité finale

L'abonné utilisera les clés et certificats pour les seuls fins désignées dans la présente PC.

2.1.3.4 Avis relatif à l'atteinte à l'intégrité de clés privées

Quand un abonné soupçonne une atteinte à l'intégrité de clés privées, il doit en aviser immédiatement l'AC de délivrance de la manière précisée par l'AC.

Quand toute autre entité soupçonne une atteinte à l'intégrité de clés privées, elle doit en aviser immédiatement l'AC de délivrance.

2.1.4 Obligations de la partie utilisatrice

Les droits et obligations d'une partie utilisatrice qui constitue un membre de l'ICP d'ADRC sont traitées dans la présente politique. Les droits et obligations d'une partie utilisatrice appartenant à une autre ICP doivent être mentionnés dans l'entente de cocertification intervenue entre les deux ICP.

2.1.4.1 Emploi de certificats à bon escient

Avant de délivrer un certificat à un abonné, une partie utilisatrice doit s'assurer qu'il se prête à l'emploi attendu.

2.1.4.2 Responsabilité de la vérification

Une partie utilisatrice doit utiliser les certificats seulement conformément à la procédure de validation du chemin de vérification précisée dans les protocoles X.509 et PKIX.

2.1.4.3 Responsabilité de la vérification de révocation

Avant d'utiliser un certificat, une partie utilisatrice doit vérifier l'état du certificat dans la LCR appropriée et actuelle conformément aux exigences énoncées à l'article 4.4.10. Dans le cadre de ce processus de vérification, la signature numérique de la LCR doit également être validée.

2.1.5 Obligations du dépôt

Le dépôt devrait être disponible pour une grande part d'une période de 24 heures. Les certificats et les LCR doivent être disponibles aux parties utilisatrices conformément aux exigences de l'article 4.4.9.

2.2 Responsabilité

2.2.1 Exigences

L'AC de délivrance s'assurera que ses services de certification et de dépôt, que la délivrance et la révocation de certificats ainsi que la délivrance de LCR sont conformes à la présente PC. Elle déploiera également tous les efforts raisonnables pour s'assurer que toutes les ALE et tous les abonnés suivront les exigences de la présente politique lors de l'utilisation de tout certificat renfermant l'IDO de la présente politique et les clés associées.

Les AC et ALE s'assureront que leurs procédures d'authentification et de validation sont mises en place de la façon décrite à l'article 3.

2.2.2 Dénis de garantis et d'obligations

La Couronne aux droits du Canada et l'ADRC n'assume aucune responsabilité de quelque nature que ce soit relativement à l'emploi des certificats ICP d'ADRC ou des paires de clés publiques/privées associées pour des fins autres que celles énoncées dans la présente PC et dans toute autre entente. Les abonnés tiendront ceux-ci indemnes et à couvert d'une telle responsabilité.

La Couronne aux droits du Canada et l'ADRC, leurs employés, fonctionnaires ou agents ne font aucune représentation ni n'émettent aucune garantie ou condition, expresses ou implicites, autres que celles énoncées expressément dans la présent PC ou dans tout autre document.

Aucun rapport de coentreprise, de partenariat, de société, d'organisme ou de fiducie n'est établi ni présumé être établi entre la Couronne est ses citoyens, ses partenaires commerciaux ou autres utilisant l'ICP d'ADRC.

2.2.3 Limitations de responsabilité

La Couronne aux droits du Canada et l'ADRC déclinent toute responsabilité de quelque nature que ce soit relativement aux attributions, aux dommages ou à toute autre réclamation ou à toute autre obligation de quelque nature que ce soit découlant d'un délit, d'un contrat ou de toute autre raison en ce qui a trait à tout service associé à la délivrance, l'emploi ou à la fiabilité d'un certificat externe d'ICP d'assurance de niveau moyen d'ADRC ou de sa paire de clés privées/publiques associée, au-delà de 50 000 $ par cas d'emploi par un abonné ou par une partie utilisatrice.

2.2.4 Autres conditions

Les dénis et limitations de responsabilité des alinéas 2.2.2 et 2.2.3 sont sujets à toute entente de cocertification ou à tout contrat signé pouvant être intervenu par la Couronne et/ou ADRC et qui pourrait en décider autrement. De tels dénis et limitations de responsabilité doivent être conformes à la présente politique de certification.

2.3 Responsabilité financière

L'AC n'émettra aucun contrat pour la fourniture de ses services d'AC.

2.4 Interprétation et exécution

2.4.1 Loi applicable

L'AC doit s'assurer que toute entente sera régie par les lois du Canada et par les lois provinciales applicables relative à l'exécution, à la construction, à l'interprétation et à la validité de la présente politique de certification. Cette entente sera régie par les lois du Canada et par les lois provinciales applicables et sera interprétée suivant ces lois, exclusion faite de leurs principes de conflits de lois.

2.4.2 Dissociabilité, survie, fusion, avis

L'AC doit s'assurer que toute entente renfermera des dispositions appropriées régissant la dissociabilité, la survie, la fusion ou l'avis.

2.4.3 Procédures de règlement de différends

Tout différend lié à la gestion des clés et des certificats entre l'ADRC et un organisme ou une personne à l'extérieur d'ADRC devrait être réglé à l'aide d'un mécanisme de règlement des différends approprié. Si possible, il faudrait résoudre par la négociation un différend. Si le différend n'est toujours pas réglé, il faudrait faire appel à un médiateur accepté par les parties prenant part au différend. Si le différend n'est toujours pas réglé, il faudrait faire appel à l'arbitrage conformément à la *Loi sur l'arbitrage commercial*.

Un différend lié à la gestion des clés et des certificats entre les ministères du GC devrait être réglé par la négociation, si possible, Si le différend n'est toujours pas réglé, il faudrait faire appel à l'AGP du GC ou, le cas échéant, à un médiateur ou à des arbitre(s) nommés par l'AGP du GC.

L'AC doit s'assurer que toute entente intervenue comporte des procédures de règlement des différends appropriées.

2.5 Droits à acquitter

L'imputation de droits à acquitter est sujette à l'autorité législative et à la politique appropriées. Un avis décrivant tout droits à acquitter imputé à un abonné ou à une partie utilisatrice doit être porté à l'attention de cette entité.

2.6 Publication et dépôt

L'AC de délivrance doit :

- inclure, dans tout certificat ou dans toute entente avec un abonné qu'elle émet, l'adresse URL d'un site Web géré par l'AC ou en son nom;
- s'assurer de la publication de sa PC, signée de façon numérique par un représentant autorisé de l'AC, sur un site Web géré par l'AC ou en son nom, dont l'emplacement doit être indiqué conformément à l'article 8;
- s'assurer, directement ou grâce à une entente avec un dépôt, que les contrôles d'accès du système d'exploitation et du dépôt seront configurés de sorte que seul le personnel autorisé de l'AC puisse écrire ou modifier la version en ligne de la PC; et
- fournir une version en texte intégral de l'ÉPC quand cela est nécessaire pour les fins de toute vérification, de toute inspection, de toute accréditation ou de tout cocertification.

Les contrôles d'accès peuvent être institués à la discrétion de l'AC en ce qui concerne les certificats ou l'état des certificats en ligne (si le dernier cas est fourni comme service par l'AC). Les certificats doivent être publiés rapidement après leur délivrance. L'AC doit s'assurer, directement ou avec l'entente avec un dépôt, de l'accès non restreint aux LCR. La publication LCR doit être conforme à l'article 4.

2.7 Inspection de conformité

Une inspection de conformité détermine si la performance de l'AC respecte les normes établies dans son ÉPC et satisfait les exigences des PC qu'elle appuie.

2.7.1 Fréquence de l'inspection de conformité

L'AC émettant les certificats conformément à la présente PC doit établir à la satisfaction de toute AC avec qui elle établit une cocertification qu'elle se conforme entièrement, par l'entremise d'une inspection de conformité, aux exigences de la présente politique :

- avant la cocertification initiale avec l'AC de l'ICP d'ADRC; et
- au minimum, douze mois par la suite.

Une inspection sur cinq doit être accomplie par un organisme externe à l'ADRC. L'ADRC et les AGP du GC peuvent, à leur discrétion, demander au commissionnaire d'ADRC de faire mener une inspection de conformité par un organisme externe à l'Agence, en tout temps.

L'AC doit certifier annuellement à l'AGP d'ADRC qu'elle s'est conformée en tout temps au cours de la période en question aux exigences de la présente politique. L'AC doit également fournir à l'AGP d'ADRC les raisons pour lesquelles l'AC ne s'est pas conformée à sa PC et énoncer toute période de non-conformité.

2.7.2 Identité/compétences de l'inspecteur de l'AC

Toute personne ou toute entité, externe au GC, qui recherche à accomplir une inspection de conformité doit présenter une expérience importante de l'ICP et des technologies de chiffrement ainsi que du fonctionnement des logiciels ICP pertinents.

2.7.3 Rapport de l'inspecteur avec l'AC vérifiée

Quand un inspecteur se trouve au GC, il doit être indépendant de l'AC.

Quand un inspecteur est externe au GC, il doit être indépendant de l'AC et doit se conformer aux dispositions du Code régissant la conduite des titulaires de charge publique en ce qui concerne les conflits d'intérêts et l'après-mandat ou le Code régissant les conflits d'intérêts et l'après-mandat s'appliquant à la fonction publique. Ne peut être nommée inspecteur en vue d'une inspection toute personne, ou tout associé ou membre de la même firme que cette personne, qui est :

i) un membre de la famille pertinente du Ministre;
ii) un membre de la famille d'un autre Ministre ou de collègues de la Chambre des communes ou du Sénat; ou
iii) employé ou membre de la famille immédiate d'une personne rappelée ci-dessus, où de tels membres de famille sont employés à un poste supérieur d'autorité dans un organisme non gouvernemental.

Aucun membre de la Chambre des communes ou du Sénat peut partager toute partie d'un contrat entre l'inspecteur et le Gouvernement du Canada, ni tout avantage en découlant.

2.7.4 Sujets traités dans l'inspection

L'inspection de conformité doit suivre les lignes directrices d'inspection instituées par l'AGP d'ADRC. Cela comprend si :

- un ÉPC décrit, en détails suffisants, les politiques et pratiques techniques, procédurales et de personnel de l'AC qui satisfont les exigences de toutes les politiques de certification appuyées par l'AC;
- l'AC met en place ces pratiques et politiques techniques, procédurales et de personnel et s'y conforme; et
- une ALE, le cas échéant, met en place ces pratiques et politiques techniques, procédurales et de personnel établies par l'AC et s'y conforme.

2.7.5 Mesures prises par suite de l'inspection

Les résultats de l'inspection doivent être présentés à l'AGP d'ADRC. En cas d'irrégularités, l'AC doit présenter un rapport à l'ADRC et aux AGP du GC quant à toute mesure que prendra l'AC en réponse au rapport d'inspection. Si l'AC ne prend aucune mesure appropriée en réponse au rapport d'inspection, l'AGP d'ADRC peut :

- faire part des irrégularités, mais permettre à l'AC de poursuivre les opérations jusqu'à la prochaine inspection prévue au calendrier; ou
- permettre à l'AC de poursuivre les opérations pour un maximum de trente jours en instance de correction de tout problème avant la révocation; ou
- diminuer le niveau d'assurance de tout cocertificat; ou
- révoquer le certificat de l'AC.

Si l'AGP d'ADRC ne prend pas de mesure, l'AGP du GC peut :

- diminuer le niveau d'assurance du cocertificat avec l'ICC; ou
- révoquer le cocertificat de l'AC avec l'ICC.

Toute décision concernant les mesures à prendre sera fondée sur la gravité des irrégularités.

2.7.6 Communication des résultats

Les AC cocertifiées avec l'ICC doivent fournir à l'AGP du GC une copie des résultats de l'inspection de conformité. Ces résultats ne seront pas rendus publics, à moins que la loi ne l'exige. La méthode et le détail de l'avis des résultats de l'inspection aux AC cocertifiées avec l'AC doivent être définis dans l'entente de cocertification entre les deux parties.

2.8 Confidentialité des renseignements

Les certificats et les LCR, ainsi que les renseignements personnels ou ministériels figurant sur ceux-ci et dans les répertoires publics ne sont pas considérés de nature délicate (de nature délicate, au sens donné dans la Politique sur la sécurité du gouvernement). Tous les autres renseignements personnels ou ministériels détenus par l'AC ou une ALE (p. ex. renseignements d'enregistrement et de révocation, événements consignés, correspondance entre l'abonné et l'AC ou l'ALE, etc.) sont considérés de nature délicate et ne doivent pas être divulgués sans le consentement préalable de l'abonné, à moins que la loi l'exige.

L'abonné doit conserver en sûreté la copie de l'abonné de sa clé privée de confidentialité. S'il divulgue celle-ci, il le fait à ses propres risques. Cependant, les clés privées de confidentialité peuvent être sauvegardées par l'AC de délivrance ou un autre tiers pour le compte de l'AC - dans ce cas les clés doivent être protégées conformément à l'article 6 -, mais elles ne doivent pas être divulguées à un autre tiers sans le consentement préalable de l'abonné ou du promoteur, à moins que la loi l'exige.

La clé privée de la signature numérique de chaque abonné ne doit être détenue que par l'abonné et doit être tenue confidentielle par lui. Toute divulgation par l'abonné est aux propres risques de ce dernier.

Les renseignements d'une inspection doivent être considérés de nature délicate et ne doivent pas être divulgués pour des fins autres que celles d'inspection ou si la loi l'exige.

Les renseignements concernant la gestion de l'AC d'un certificat de signature numérique d'un abonné ne peuvent être divulgués qu'à l'abonné, qu'au parrain ou que si la loi l'exige.

Toute demande de divulgation de renseignements doit être signée et délivrée à l'AC.

Toute divulgation de renseignements est sujette aux exigences de la *Loi sur la protection des renseignements personnels,* de la *Loi sur l'accès à l'information*, de toute autre législation et de toute autre politique applicable du Gouvernement du Canada.

2.9 Droits de propriété intellectuelle

Aucune disposition.

3. Identification et authentification

3.1 Enregistrement initial

3.1.1 Types de noms

Chaque entité doit détenir un Nom distinctif (ND) X.501 facile à distinguer et unique dans le champ de nom de sujet du certificat, conformément à l'ICPX, Partie 1. Chaque entité peut utiliser un nom de rechange grâce au champ **SubjectAlternateName**, qui doit également être conforme à l'ICPX, Partie 1. Le ND doit se présenter sous la forme d'une chaîne printableString X.501 et ne doit pas être vide.

3.1.2 Obligation d'utiliser des noms significatifs

Le contenu des champs Subject et Issuer de chaque certificat doit comporter une association au nom authentifié de l'entité. Dans le cas de personnes, le Nom distinctif relatif (NDR) devrait être une combinaison du prénom, du nom et, en option, des initiales. Ce NDR peut également comprendre un poste ou un rôle organisationnel. Dans le cas d'autres entités, le NDR représentera le nom légal authentifié de l'entité; il n'est pas nécessaire qu'il comprenne le nom de l'abonné.

Quand un certificat renvoie à un rôle ou à un poste, le certificat doit également renfermer l'identité de la personne détenant ce rôle ou ce poste.

Un certificat délivré pour un dispositif ou une application doit inclure dans le ND le nom de la personne ou de l'organisme responsable de ce dispositif ou de cette application.

3.1.3 Règles d'interprétation des diverses formes de noms

Aucune disposition.

3.1.4 Unicité des noms

Les noms distinctifs doivent être uniques pour toutes les entités finales d'une AC. Pour chaque entité finale, des nombres ou des lettres supplémentaires peuvent être annexés à **commonName** afin de s'assurer de l'unicité du NDR. La capacité des identificateurs uniques à distinguer les abonnés aux noms identiques ne sera pas appuyée.

3.1.5 Procédure de règlement des différends relativement à la revendication des noms

L'AC se réserve le droit de prendre toutes les décisions relativement aux noms des entités dans tous les certificats attribués. Une partie demandant un certificat doit démontrer son droit d'utiliser un nom particulier.

En cas de différend au sujet d'un nom dans un dépôt non sous le contrôle de l'AC, cette dernière doit s'assurer qu'il existe une procédure de règlement des différends relativement à la revendication des noms dans son entente avec ce dépôt.

3.1.6 Reconnaissance, authentification et rôles des marques de commerce

L'emploi de marques de commerce sera réservé aux détenteurs de marques de commerce déposées.

3.1.7 Méthode visant à prouver la possession d'une clé privée

Avant la délivrance d'un certificat de vérification, l'AC de délivrance et l'entité finale confirmeront leur identité respective par l'emploi d'un secret partagé.

Le protocole de transfert de clés décrit dans le protocole de gestion de certificats ICPX se prête à cette exigence.

3.1.8 Authentification de l'identité d'un organisme

La demande d'une organisation en vue de devenir un abonné peut être effectuée par la personne autorisée à agir au bon de l'abonné éventuel.

L'identification et l'authentification de l'abonné éventuel doivent se faire à l'aide d'un des moyens suivants :

- l'AC ou l'ALE doit examiner les copies notariées de la documentation attestant de l'existence de l'organisation;
- si l'organisme a déjà établi l'identité de l'organisation à l'aide d'un processus satisfaisant l'AC et qu'aucune modification n'a été apportée dans les renseignements présentés, l'AC ou l'ALE et l'abonné éventuel peuvent utiliser ce renseignement partagé de façon privée.

L'AC ou l'ALE doit aussi vérifier l'identité et l'autorité de la personne agissant au bon de l'abonné éventuel, ainsi que son autorité de recevoir les clés pour le compte de l'organisation.

L'AC ou l'ALE doit tenir un dossier du type et des détails d'identification utilisés.

3.1.9 Authentification de l'identité d'une personne

La demande d'une personne en vue de devenir un abonné peut être effectuée par la personne ou par une autre personne ou par un autre organisme autorisé à agir au bon de l'abonné éventuel.

L'identification et l'authentification de la personne doivent se faire à l'aide d'un des moyens suivants :

- l'AC ou l'ALE compareront l'identité de la personne avec deux pièces d'identification (copies notariées ou originaux). Au moins l'une d'elles doit être l'insigne d'identification du gouvernement présentant une photographie; ou
- si l'organisme a déjà établi l'identité d'une personne à l'aide d'un processus satisfaisant l'AC et qu'aucune modification n'a été apportée dans les renseignements présentés, l'AC ou l'ALE et la personne peuvent utiliser ce renseignement partagé de façon privée.

L'AC ou l'ALE doit tenir un dossier du type et des détails d'identification utilisés.

3.1.10 Authentification de dispositifs ou d'applications

Une demande de dispositif ou d'application en vue de devenir une entité finale peut être déposée par une personne ou un organisme auquel est attribuée la signature du dispositif ou de l'application aux fins de comptabilité et de responsabilité.

L'identification et l'authentification du demandeur doivent suivre les instructions des alinéas 3.1.8 ou 3.1.9 comme si cette personne ou cet organisme déposait une demande de certificat en son nom propre.

L'AC ou l'ALE doit également vérifier l'identité de la personne ou de l'organisme demandeur et son autorité à recevoir les clés pour ce dispositif ou cette application.

L'AC ou l'ALE doit tenir un dossier du type et des détails d'identification utilisés.

3.2 Authentification pour le renouvellement routinier d'une clé

Une demande de renouvellement ne peut être déposée que par l'entité au nom de laquelle les clés ont été délivrées. Toutes les demandes de renouvellement doivent être authentifiées par l'AC et la réponse subséquente doit être authentifiée par l'entité. On y parvient par une méthode en ligne conformément à l'ICPX, Partie 3 – Protocole de gestion de certificats. Une entité demandant un renouvellement peut authentifier la demande à l'aide de sa paire de clés de signatures numériques valide. Advenant l'expiration de l'une des clés, la demande de renouvellement doit être authentifiée de la même façon que pour un enregistrement initial.

3.3 Authentification pour le renouvellement d'une clé par suite d'une révocation

Si les renseignements contenus dans un certificat ont changé ou qu'il existe une atteinte à l'intégrité connue ou soupçonnée de la clé privée, l'AC doit authentifier un renouvellement de la même façon que pour un enregistrement initial. Toute modification apportée aux renseignements contenus dans un certificat doit être vérifiée par l'AC ou par l'ALE autorisée à agir au nom de l'AC avant la délivrance du certificat.

3.4 Authentification d'une demande de révocation

L'AC ou une ALE agissant en son nom doit authentifier une demande de révocation d'un certificat, L'AC doit établir et rendre public le processus à l'aide duquel il traite de telles demandes et les moyens par lesquels il établira la validité de la demande.

Les demandes de révocation de certificats doivent être consignées.

4. Exigences opérationnelles

4.1 Demande de certificats

L'AC doit s'assurer que toutes les procédures et exigences en ce qui concerne une demande de certificat sont définies dans l'ÉPC ou dans un document disponible publiquement. Les demandes en lots au nom d'entités finales sont permises seulement par les personnes autorisées à déposer de telles demandes.

L'AC doit s'assurer que chaque demande est accompagnée des effets suivants :

- preuve de l'identité de l'entité finale;
- preuve de l'autorisation de tout attribut de certificat demandé;
- entente signée par l'entité finale relativement aux conditions régissant l'utilisation du certificat;

Une demande de certificat n'oblige pas l'AC à délivrer un certificat.

4.1.1 Demande de cocertificats

L'ICC ou l'AC désignera toutes les procédures et exigences en ce qui concerne une demande de cocertificat dans ses procédures de cocertification.

Une AC demandant une cocertification par l'ICC ou l'AC doit s'assurer que chaque demande est accompagnée des effets suivants :

- politique de certification;
- rapport d'inspection de vérification validant le niveau d'assurance énoncé dans le PC;
- clé de vérification publique produite par l'AC.

Une demande de cocertificat n'oblige pas l'ICC ou l'AC à délivrer un cocertificat.

4.2 Délivrance de certificats

La délivrance et la publication d'un certificat par l'AC indique une approbation complète et finale de la demande de certificat par l'AC.

4.3 Acceptation de certificats

L'AC doit s'assurer qu'une entité reconnaît l'acceptation d'un certificat. Pour un dispositif ou une application, cette reconnaissance peut être accomplie par la personne ou l'organisme responsable du dispositif ou de l'application.

4.4 Suspension et révocation de certificats

4.4.1 Circonstances de révocation

Un certificat peut être révoqué :

- quand tout renseignement du certificat change;
- quand on soupçonne une atteinte à l'intégrité de la clé privée ou que l'on en est assuré;
- quand on soupçonne une atteinte à l'intégrité du support de stockage de la clé privée ou que l'on en est assuré.

L'AC peut, à sa discrétion, révoquer un certificat quand une entité ne se conforme pas aux obligations énoncées dans la présente PC, dans l'ÉPC, dans toute entente ou dans toute loi applicable.

Quand l'AC est cocertifiée avec l'ICC, cette dernière doit révoquer un cocertificat :

- quand tout renseignement du certificat change;
- quand on soupçonne une atteinte à l'intégrité de la clé privée ou que l'on en est assuré;
- quand on soupçonne une atteinte à l'intégrité du support de stockage de la clé privée ou que l'on en est assuré.

L'AGP du GC ou d'ADRC peut, à sa discrétion, révoquer un cocertificat quand une AC ne se conforme pas aux obligations énoncées dans la présente PC, dans l'ÉPC connexe, dans toute entente ou dans toute loi applicable.

4.4.2 Qui peut demander une révocation

La révocation d'un certificat peut être demandée uniquement par les personnes suivantes :

- l'abonné au nom duquel a été délivré le certificat;
- la personne ou l'organisme qui a déposé la demande de certificat au nom du dispositif ou de l'application;
- le parrain;
- le personnel de l'AC de délivrance;
- le personnel d'une ALE associée à l'AC de délivrance.

La révocation d'un cocertificat peut être demandée uniquement par les personnes suivantes :

- l'AC au nom duquel a été délivré le cocertificat;
- le personnel exploitant l'ICC;
- l'AGP du GC ou d'ADRC.

4.4.3 Procédure de demande de révocation

L'AC doit s'assurer que toutes les procédures et exigences relatives à la révocation d'un certificat sont définies dans l'ÉPC ou autrement rendues publiques. Une demande de révocation authentifiée et toute mesure résultante prise par l'AC doivent être consignées et conservées. Dans le cas où un certificat est révoqué, la justification entière de la révocation doit être documentée également.

Si le certificat d'une entité est révoqué, la révocation sera publiée dans la LCR appropriée. Quand un cocertificat est révoqué, la révocation sera publiée dans la LCAR de l'AC de délivrance.

4.4.4 Délai de grâce pour une demande de révocation

Toute mesure prise par suite d'une demande de révocation d'un certificat sera immédiatement lancée si la demande est reçue au cours des heures ouvrables locales de l'AC ou dans les 12 (douze) heures de la réception.

4.4.5 *Circonstances de suspension de certificat (désactivation du compte de l'abonné)*

L'AC de l'ADRC peut suspendre (désactiver) le compte d'abonnés qui partent pour une période prolongée, par exemple dans le cas d'un congé de maternité. L'AC de l'ADRC peut aussi suspendre les certificats d'abonnés pendant la vérification des demandes de révocation.

4.4.6 *Qui peut demander une suspension (désactivation)*

Les personnes suivantes peuvent présenter une demande de suspension (désactivation) :

- Les abonnés;
- La personne qui a déposé la demande de certificat au nom du dispositif ou de l'application;
- Le parrain;
- Les agents de l'ALE, au nom d'un parrain ou d'un abonné;
- Le personnel de l'AC de l'ADRC.

4.4.7 *Procédure de demande de suspension (désactivation)*

L'abonné ou le parrain doit soumettre la demande à un agent de l'ALE par un message électronique portant une signature numérique. L'agent de l'ALE utilisera le même moyen pour transmettre la demande à l'AC de l'ADRC. Quand la demande parvient à l'agent de l'ALE, ce dernier doit la soumettre directement à l'AC de l'ADRC par un message électronique portant une signature numérique.

La procédure de traitement de la demande de suspension est la suivante :

- La demande est soumise à l'AC de l'ADRC conformément aux directives ci-dessus;

- La signature numérique de la demande est vérifiée;
- Si la demande est justifiée, les certificats de l'abonné sont suspendus (désactivés) et l'agent de l'ALE en est avisé;
- L'agent de l'ALE informe les abonnés de la suspension (désactivation) de leurs certificats;
- Les certificats sont suspendus (désactivés) quand l'AC de l'ADRC reçoit la demande.

Les abonnés doivent se présenter en personne à un agent de l'ALE pour demander le rétablissement des certificats suspendus (désactivés).

4.4.8 *Limites de la période de suspension (désactivation)*

Il n'y a aucune limite. Le certificat deviendra périmé conformément à l'alinéa 6.3.2.

4.4.9 Fréquence de délivrance d'une LCR

L'AC doit s'assurer qu'elle émet une LCR à jour au moins toutes les douze heures. L'AC doit également s'assurer que la délivrance de sa LCR est synchronisée avec toute synchronisation de répertoires, afin d'assurer l'accessibilité de la LCR la plus récente aux parties utilisatrices. Si un certificat est révoqué en raison de l'atteinte à l'intégrité d'une clé, la LCR à jour sera délivrée immédiatement.

4.4.10 Exigences de vérification d'une LCR

Une partie utilisatrice doit vérifier l'état de tous les certificats dans la chaîne de validation des certificats relativement aux LCR et aux LCAR actuels avant leur emploi. Une partie utilisatrice doit également vérifier l'authenticité et l'intégrité des LCR et des LCAR.

4.4.11 Disponibilité de la vérification de la révocation/de l'état en ligne

L'ICP d'ADRC n'appuie pas actuellement la disponibilité de la vérification de la révocation/de l'état en ligne.

4.4.12 Exigences de la vérification de révocation en ligne

Sans objet.

4.4.13 Autres formes d'avis de révocation disponibles

Sans objet.

4.4.14 Vérification des exigences pour les autres formes d'avis de révocation

Sans objet.

4.4.15 Exigences spéciales : atteinte à l'intégrité de clés

En cas d'atteinte à l'intégrité réelle ou soupçonnée de la clé de signature de toute autre entité, l'entité doit immédiatement en aviser l'AC de délivrance.

L'AC doit s'assurer que son ÉPC ou un document disponible publiquement et les ententes appropriées comportent des dispositions décrivant dans les grandes lignes les moyens dont elle se servira pour fournir un avis d'atteinte à l'intégrité réelle ou soupçonnée.

4.5 Procédures de vérification de la sécurité de systèmes

4.5.1 Types d'événements enregistrés

L'AC devrait consigner dans les fichiers de consignation de vérification tous les événements liés à la sécurité du système de l'AC. Voici des exemples d'événements :

- démarrage et arrête du système;
- démarrage et arrêt de l'application de l'AC;

- tentatives de création, de suppression, de définition de mots de passe ou de modification des privilèges du système de l'agent maître de l'ICP, de l'agent de l'ICP ou de l'administrateur de l'ICP;
- modifications aux détails et/ou aux clés de l'AC;
- modifications aux politiques de création de certificats, p. ex. période de validité;
- tentatives d'ouverture et de fermeture de séance;
- tentatives non autorisées d'accès réseau au système de l'AC;
- tentatives non autorisées d'accès aux fichiers du système;
- production des clés de l'entité propres et subalternes;
- création et révocation de certificats;
- tentatives d'initialisation, de suppression, de validation et d'invalidation d'abonnées ainsi que de mise à jour et de récupération de leurs clés;
- opérations de lecture-écriture échouées du certificat et du répertoire des LCR.

Tous les journaux, électroniques ou manuels, devraient renfermer la date et l'heure de l'événement ainsi que l'identité de l'entité à l'origine de l'événement.

L'AC devrait également recueillir et consolider, de façon électronique ou manuelle, les renseignements sur la sécurité non produits par le système de l'AC, tels :

- journaux d'accès physique;
- modifications et maintenance de la configuration du système;
- modifications du personnel;
- rapports d'écart et d'atteinte à l'intégrité;
- dossiers sur la destruction des supports renfermant le matériel sur les clés, les données d'activation ou les renseignements personnels sur l'abonné.

L'AC doit s'assurer que l'ÉPC indique quels renseignements sont consignés.

Pour faciliter la prise de décisions, toutes les ententes et la correspondance liée aux services de l'AC devraient être recueillies et consolidées, de façon électronique ou manuelle, dans un seul emplacement.

4.5.2 Fréquence du traitement des journaux de vérification

L'AC doit s'assurer que ses journaux de vérification sont examinés par le personnel de l'AC au moins une fois toutes les semaines et que tous les événements d'importance sont expliqués dans un sommaire des journaux de vérification. De tels examens supposent la vérification que le journal n'a pas été falsifié et la brève inspection de toutes les entrées de journal, avec une enquête plus approfondie de toute alerte ou irrégularité dans les journaux. Les journaux électroniques et le manuel à l'appui de l'AC et de l'ALE devraient être comparés quand tout mesure est jugée douteuse.

Les mesures prises par suite de ces examens doivent être documentées.

4.5.3 Période de conservation du journal de vérification

L'AC doit conserver ses journaux de vérification sur le site au moins tous les deux mois et les conserver par la suite de la façon décrite à l'article 4.6.

4.5.4 Protection du journal de vérification

Le système des journaux de vérification électroniques doivent comprendre des mécanismes de protection de tous les fichiers de journaux contre la consultation, la modification et la suppression non autorisées.

Les renseignements sur la vérification manuelle doivent être protégés contre la consultation, la modification et la destruction non autorisées.

4.5.5 Procédures de sauvegarde du journal de vérification

Les journaux de vérification et les sommaires de vérification doivent être sauvegardés ou copiés sous forme manuelle.

4.5.6 Système de collecte pour la vérification

L'AC doit désigner ses systèmes de collecte de vérification dans l'ÉPC.

4.5.7 Avis relatif à l'événement à l'origine du sujet

Quand un événement est consigné par le système de collecte de vérification, il n'est pas nécessaire d'en donner avis à la personne, à l'organisme, au dispositif ou à l'application ayant causé l'événement.

4.5.8 Évaluations de la vulnérabilité

Les événements du processus de vérification sont consignés, en partie, afin de surveiller les vulnérabilités du système. L'AC doit s'assurer qu'une évaluation de la vulnérabilité est menée, examinée et révisée par suite d'un examen de ces événements surveillés.

4.6 Archivage des dossiers

Les certificats de signature numérique, les clés privés de confidentialité stockées par l'AC ainsi que les LCAR et LCR produites par l'AC doivent être conservés pendant au moins un an après l'expiration du matériel sur les clés. Cette exigence ne comprend pas la sauvegarde des clés privées de signature.

Les renseignements de vérification dont les détails sont fournis à l'article 4.5, les ententes avec les abonnés ainsi que tout renseignement d'identification et d'authentification devraient être conservés pendant au moins six ans.

Les clés privées de confidentialité sauvegardées par l'AC doivent être protégées à un niveau de protection matériel et de chiffrement égal ou supérieur à celui en place au site de l'AC.

Une deuxième copie de tout matériel conservé ou sauvegardé doit être conservée dans un emplacement autre que le site de l'AC et doit être protégée par sécurité matérielle seulement ou par combinaison de dispositifs matériels et de chiffrement. Tout site secondaire de la sorte doit fournir une protection adéquate contre les dangers de l'environnement comme la température, l'humidité et le magnétisme.

L'AC devrait vérifier l'intégrité des sauvegardes une fois tous les six mois.

La matériel stocké hors site doit être vérifié de façon périodique relativement à l'intégrité des données.

Outre les points susmentionnés, les renseignements conservés ou sauvegardés par l'AC peuvent être sujets à la *Loi sur les archives nationales*.

4.7 Renouvellement de clés

Un abonné peut uniquement présenter une demande de renouvellement de sa paire de clés dans les trois mois précédant l'expiration de l'une des clés, pourvu que le certificat précédent n'ait pas été révoqué. Un abonné, l'AC ou l'ALE peut lancer ce processus de renouvellement de clés. Le renouvellement automatisé des clés est permis. L'AC doit s'assurer que les détails du processus sont indiqués dans son ÉPC.

Les abonnés sans clés valides doivent être authentifiés de nouveau par l'AC ou l'ALE de la même façon que celle utilisée pour le dossier initial.

Si le certificat d'un abonné a été révoqué par suite de non-conformié, l'AC doit vérifier si des raisons ont été mentionnées relativement à la non-conformité, à sa satisfaction, avant la nouvelle délivrance d'un certificat.

Il n'est pas possible de renouveler les clés à l'aide d'une clé de signature numérique expirée.

4.8 Atteinte à l'intégrité et reprise après sinistre

4.8.1 Corruption des ressources informatiques, des logiciels et/ou des données

L'AC doit établir les procédures de continuité des opérations donnant les grandes lignes des étapes à suivre en cas de corruption ou de perte des ressources informatiques, des logiciels et/ou des données. Si un dépôt n'est pas sous le contrôle de l'AC, l'AC doit s'assurer que toute entente avec le dépôt comporte des procédures de continuité des opérations établies et documentées par le dépôt.

4.8.2 Révocation du certificat public d'une entité

En cas de nécessité d'une révocation du certificat de confidentialité de l'AC, le numéro de série du certificat devrait être indiquée sur une LCR appropriée.

4.8.2.1 Déclassement du certificat public d'une entité

Le numéro de série du certificat devrait être indiquée sur une LCR appropriée.

En cas de nécessité d'un déclassement du certificat de confidentialité de toute autre entité, l'AC ou l'ALE doit en aviser l'abonné de la façon décrite dans son ÉPC et dans l'entente avec l'abonné.

4.8.3 Atteinte à l'intégrité de la clé d'une entité

En cas d'atteinte à l'intégrité réelle ou soupçonnée de la clé de déchiffrement privée de l'AC, ce dernier doit immédiatement en aviser l'AGP d'ADRC.

En cas d'atteinte à l'intégrité réelle ou soupçonnée de la clé de déchiffrement privée de toute autre entité, cette dernière doit immédiatement en aviser l'AC de délivrance.

L'AC doit s'assurer que son ÉPC et les ententes appropriées comportent des dispositions décrivant dans les grandes lignes les moyens dont elle se servira pour fournir un avis d'atteinte à l'intégrité réelle ou soupçonnée.

4.8.4 Installation sécuritaire après un désastre naturel ou un désastre d'un autre type

L'AC doit établir un plan de reprise après sinistre décrivant dans les grandes lignes les étapes à suivre pour rétablir une installation sécuritaire en cas de désastre naturel ou autre. Si un dépôt n'est pas sous le contrôle de l'AC, l'AC doit s'assurer que toute entente avec le dépôt comporte un plan de reprise après sinistre établi et documenté par le dépôt.

4.9 Cessation de l'AC

En cas de cessation des activités de l'AC, l'AC doit en aviser immédiatement les abonnés à la fin des activités et prendre des dispositions pour assurer la conservation continue des clés et des renseignements la concernant. L'AC doit également aviser toutes les AC avec qui est détient des cocertificats.

En cas de modification à la gestion des activités de l'AC, l'AC doit en aviser toutes les entités à qui elle a délivré des certificats et toutes les AC avec qui elle détient des cocertificats.

En cas de transfert des activités de l'AC à une autre AC active à un niveau d'assurance inférieur, les certificats délivrés par l'AC dont les activités sont transférées doivent être révoqués par une LCR signé par cette AC avant le transfert.

Les archives de l'AC doivent être conservées de la façon et pour la durée décrites à l'article 4.6.

5. Sécurité matérielle, procédurale et du personnel

5.1 Contrôles matériels

5.1.1 Emplacement et construction du site ainsi qu'accès physique à celui-ci

Le site de l'AC doit :

- satisfaire au moins toutes les exigences relatives à une zone sécuritaire;
- être surveillé de façon manuelle ou électronique en ce qui a trait aux intrusions non autorisées, en tout temps;
- s'assurer que l'accès par escorte au serveur de l'AC est limité au personnel désigné sur une liste d'accès;
- s'assurer que le personnel ne figurant pas sur la liste d'accès est escorté et supervisé de façon appropriée;
- s'assurer qu'un journal d'accès au site est conservé et inspecté de façon périodique; et
- s'assurer que tout support retirable et que tout document renfermant des renseignements textuels de nature délicate sont stockés dans des contenants énumérés dans le Guide sur le matériel de sécurité ou dans des contenants de résistance équivalente à ceux-ci.

Tous les sites des ALE doivent être situés dans des secteurs qui satisfont les contrôles nécessaires pour une zone de réception.

Si le poste de travail d'une ALE sert à la gestion en ligne d'une entité avec l'AC, ce poste doit être situé :

- dans une zone d'opérations; ou
- dans une zone de réception surveillée, ou protégée par dispositif de sécurité pendant sa non-surveillance.

L'AC s'assurera que l'exploitation du site d'ALE offre la protection appropriée en matière de sécurité du module de chiffrement, de tous les logiciels du système et de la clé privée de l'administrateur de l'ALE. L'AC doit mener une évaluation de la menace et des risques. Par exemple, le module de chiffrement et la clé privée de l'administrateur de l'ALE pourraient être stockés dans un contenant ou un coffre-fort sécuritaire.

Si un NIP ou mot de passe est consigné, il doit être stocké dans un contenant sécuritaire accessible seulement au personnel autorisé.

Les abonnés ne doivent pas laisser sans surveillance leurs postes de travail quand le chiffrement se trouve dans un état non verrouillé (c.-à-d. quand le NIP ou le mot de passe a été entré). Un poste de travail qui renferme les clés privées sur un lecteur de disque dur doit être pourvu d'un dispositif de sécurité ou être protégé physiquement par un produit de contrôle d'accès approprié.

5.1.2 Alimentation et climatisation d'air

L'AC doit s'assurer que les installations d'alimentation et de climatisation d'air suffisent à l'exploitation du système de l'AC.

5.1.3 Exposition à l'eau

L'AC doit s'assurer que le système de l'AC est protégé contre l'exposition à l'eau.

5.1.4 Prévention des incendies et protection contre ceux-ci

L'AC doit s'assurer que le système de l'AC est protégé par un système d'extinction incendie.

5.1.5 Stockage des supports

L'AC doit s'assurer que les supports de stockage utilisés par le système de l'AC sont protégés contre les dangers de l'environnement comme la température, l'humidité et le magnétisme.

5.1.6 Élimination des données

Tous les supports utilisés pour le stockage des renseignements comme les clés, les données d'activation ou les fichiers de l'AC doivent être nettoyées ou détruites avant leur libération en vue de leur élimination.

5.1.7 Sauvegarde à l'extérieur du site

L'AC doit s'assurer que les installations utilisées pour la sauvegarde hors site, le cas échéant, sont du même niveau de sécurité que le site primaire de l'AC.

5.2 Contrôles procéduraux

5.2.1 Rôles confiés

5.2.1.1 Rôles confiés à l'AC

L'AC doit s'assurer d'une séparation des tâches pour les fonctions critiques de l'AC afin d'empêcher une personne d'utiliser de façon malveillante le système de l'AC sans détection. L'accès de chaque utilisateur au système doit être limité aux gestes que chacun doit poser dans l'exécution de ses responsabilités.

L'AC devrait fournir au moins trois rôles distincts du personnel pour l'ICP, pour distinguer les activités quotidiennes du système de l'AC, la gestion et la vérification de ces activités ainsi que la gestion des modifications d'importance des exigences, y compris les politiques, les procédures ou le personnel. La division des responsabilités entre les trois rôles devrait être comme suit :

- Utilisateur maître de l'ICP
  - configuration et maintenance du matériel et des logiciels du système de l'AC;
  - commencement et cessation des services de l'AC.

- Agent de l'ICP
  - gestion des opérateurs de l'ICP et des autres agents de l'ICP;
  - configuration des politiques en matière de sécurité de l'AC;
  - vérification des journaux de vérification;
  - vérification de la conformité à la PC et à l'ÉPC.

- Administrateur de l'ICP
  - gestion du processus d'initialisation des abonnés;
  - création, renouvellement ou révocation des certificats;
  - distribution des jetons (le cas échéant).

Comme mesure de rechange, une division des responsabilités est permise dans la mesure où elle offre le même degré de résistance à une attaque intérieure.

Seul le personnel responsable des tâches décrites pour l'utilisateur maître de l'ICP et pour l'administrateur du système devrait avoir accès aux logiciels contrôlant l'exploitation de l'AC.

5.2.1.2 Rôles confiés à l'ALE

L'AC doit s'assurer que le personnel de l'ALE comprend ses responsabilités pour l'identification et l'authentification des abonnés éventuels et pour l'accomplissement des fonctions suivantes :

- acceptation des demandes d'abonnement, de modification de certificats, de révocation de certificats et de récupération de clés;
- vérification de l'identité et des autorisations des demandeurs;
- transmission des renseignements sur le demandeur à l'AC;
- fourniture de codes d'autorisation pour la création de certificats et pour l'échange de clés en ligne.

L'AC peut permettre que toutes les tâches liées aux fonctions de l'ALE soient accomplies par une seule personne.

5.2.2 Nombre de personnes nécessaires par tâche

L'AC doit s'assurer qu'aucune personne ait accès aux clés privées de l'abonné stockées par l'AC. Au moins deux personnes, qui feront appel de préférence à la technique de connaissance répartie, comme des mots de passe jumelés, doivent accomplir toute récupération de clés.

Le contrôle par des utilisateurs multiples est également nécessaire pour la production des clés de l'AC, de la façon décrite à l'alinéa 6.2.2.

Toutes les autres tâches connexes aux rôles de l'AC peuvent être accomplies par une personne fonctionnant de façon autonome. L'AC doit s'assurer que toute vérification qu'elle emploie assure la surveillance de toutes les activités accomplies par les détenteurs de rôles privilégiés dans l'AC.

5.2.3 Identification et authentification pour chaque rôle

Tout le personnel de l'AC doit faire vérifier son identité et son autorisation avant :

- d'être inclus dans la liste d'accès au site de l'AC;
- d'être inclus dans la liste d'accès matériel au système de l'AC;
- de recevoir un certificat relativement à l'accomplissement de son rôle dans l'AC;
- de recevoir un compte sur le système de l'ICP.

Chacun de ces certificats et comptes (à l'exception des certificats de signature de l'AC) :

- doivent être directement attribuables à une personne;
- ne doivent pas être partagés;
- doivent être limités aux gestes autorisés pour ce rôle, par l'emploi de logiciels, du système d'exploitation et des contrôles de procédures de l'AC.

Les activités de l'AC doivent être protégées par des dispositifs de sécurité, à l'aide de mécanismes comme l'authentification et le chiffrement prononcés fondés sur des jetons, quand l'accès a lieu par réseau par réseau partagé.

5.3 Contrôles de sécurité du personnel

L'AC doit s'assurer que tout le personnel accomplissant des tâches relativement à l'exploitation de l'AC ou de l'ALE :

- est nommé par écrit;
- est lié par contrat ou acte aux conditions du poste qu'il doit occuper;
- a reçu une formation approfondie relativement aux tâches qu'il doit accomplir;
- est lié par acte ou contrat à ne pas divulguer des renseignements de nature délicate liés à la sécurité de l'AC ou des renseignements sur l'abonné; et
- ne reçoit aucune responsabilité pouvant constituer un conflit d'intérêts avec les tâches de l'AC ou de l'ALE.

5.3.1 Exigences en matière de connaissances, de compétences, d'expérience et d'habilitation de sécurité

L'AC doit s'assurer que tout le personnel accomplissant des tâches relativement à l'exploitation de l'AC détient une habilitation de sécurité de niveau II. L'AC doit s'assurer que tout le personnel exploitant le poste de travail d'une ALE aux fins de gestion en ligne d'une entité avec l'AC détient une VAF (Vérification approfondie de la fiabilité) conformément à la politique en matière de sécurité d'ADRC.

5.3.2 Procédures de vérification des connaissances

Toutes les vérifications des connaissances doivent être accomplies conformément à la Politique sur la sécurité du gouvernement.

5.3.3 Exigences en matière de formation

L'AC doit s'assurer que tout le personnel accomplissant des tâches relativement à l'exploitation de l'AC ou de l'ALE reçoit une formation approfondie en ce qui a trait aux aspects suivants :

- principes et mécanismes de sécurité de l'AC/ALE;
- toutes les versions logicielles de l'ICP en cours d'emploi sur le système de l'AC;
- toutes les tâches de l'ICP qu'il doit accomplir; et
- procédures de reprise après sinistre et de continuité des opérations.

5.3.4 Fréquence et exigences en matière de renouvellement de la formation

Les exigences énoncées à l'alinéa 5.3.3 doivent être tenues à jour afin de tenir compte des modifications apportées au système de l'AC. La formation de recyclage doit être menée suivant les besoins et l'AC doit examiner ces exigences au moins une fois l'an.

5.3.5 Rotation des emplois

Aucune disposition.

5.3.6 Sanctions dans le cas de gestes non autorisés

En cas de geste non autorisé réel ou soupçonné par une personne accomplissant les tâches relatives à l'exploitation de l'AC ou de l'ALE, l'AC prendra immédiatement les mesures visant la suspension d'accès au système de l'AC.

5.3.7 Personnel à contrat

L'AC doit s'assurer que l'accès du personnel à contrat au site de l'AC est conforme à l'alinéa 5.1.1.

5.3.8 Documentation fournie au personnel

L'AC doit mettre à la disposition du personnel de l'AC et de l'ALE les politiques relatives aux certificats qu'elle appuie, son ÉPC ainsi que tout acte, toute politique ou tout contrat propre au poste du personnel.

6. Contrôles de sécurité techniques

6.1 Production et installation de paires de clés

6.1.1 Production de paires de clés

Chaque paire de clés de confidentialité doit être produite à l'aide de l'algorithme approuvé par l'AGP d'ADRC.

6.1.2 Délivrance de clés privées à une entité

Si la clé de déchiffrement privée n'est pas produite par le détenteur éventuel du certificat, elle doit être délivrée à l'entité par transaction en ligne conformément au protocole de gestion de certificats ICPX-3 ou par une façon aussi sécuritaire approuvée par l'AGP d'ADRC.

6.1.3 Délivrance de clés publiques au délivreur d'un certificat

Si la clé de chiffrement publique n'est pas produite par l'AC, elle doit être délivrée à l'AC par transaction en ligne conformément au protocole de gestion de certificats ICPX-3 ou par une façon aussi sécuritaire approuvée par l'AGP d'ADRC.

6.1.4 Délivrances de clés publiques de l'AC aux utilisateurs

La clé de vérification publique de l'AC doit être délivrée au détenteur de certificat éventuel par transaction en ligne conformément au protocole de gestion de certificats ICPX-3 ou par façon aussi sécuritaire approuvée par l'AGP d'ADRC.

6.1.5 Taille des clés asymétriques

L'AC doit s'assurer que les paires de clés pour toutes les entités de l'ICP sont de l'algorithme RSA ou DSA 1024 bits ou de l'algorithme RSA 2048 bits.

6.1.6 Production de paramètres des clés publiques

Une AC qui utilise l'algorithme DSA doit produire des paramètres conformément à la PUB FIPS 186.

6.1.7 Vérification de la qualité des paramètres

Sans objet.

6.1.8 Production de clés par matériel/logiciel

Les paires de clés de signature numérique de l'AC doivent être produites dans un module de chiffrement matériel. Les paires de clés pour toutes les autres entités peuvent être produites dans un module de chiffrement matériel ou logiciel.

6.1.9 Usages visés des clés (conformément au champ X.509v3)

Les clés peuvent être utilisées pour l'échange et l'établissement des clés utilisées en vue de la confidentialité des sessions et des données.

Le champ **KeyUsage** du certificat doit être utilisé conformément à l'ICPX-1, Certificat, et au profil des LCR. L'une des valeurs suivantes de KeyUsage doit figurer dans tous les certificats :

- **KeyEncipherment**, ou
- **dataEncipherment**.

Aucune autre valeur ne doit être présente.

6.2 Protection de clés privées

Le détenteur de certificat doit protéger ses clés privées contre la divulgation.

6.2.1 Normes pour le module de chiffrement

Consultez l'article 6.8 de la présente politique.

6.2.2 Contrôle de clés privées par plusieurs personnes

Il doit y avoir un contrôle par plusieurs personnes pour les activités de production de clés de l'AC. Deux membres du personnel accomplissant les tâches associées aux rôles de l'utilisateur de l'agent de l'ICP doivent participer ou être présentes.

Il doit y avoir un contrôle par plusieurs personnes pour la récupération des clés privées. Deux membres du personnel accomplissant les tâches associées aux rôles de l'utilisateur maître de l'ICP, de l'agent de l'ICP ou de l'administrateur de l'ICP doivent participer ou être présentes.

6.2.3 Entiercement de clés privées

Sans objet.

6.2.4 Sauvegarde de clés privées

L'AC de délivrance peut sauvegarder les clés privées. Une entité peut aussi sauvegarder sa propre clé. Les clés sauvegardées doivent être stockées sous forme chiffrée ainsi que protégées à un niveau supérieur ou égal à celui énoncé pour la version primaire de la clé.

6.2.5 Archivage de clés privées

Consultez l'article 4.6 de la présente politique.

6.2.6 Entrée de clés privées dans le module de chiffrement

Si la clé de déchiffrement privée n'est pas produite dans le module cryptographique de l'entité, elle doit y être entrée conformément au protocole de gestion de certificats ICPX-3 ou par façon aussi sécuritaire approuvée par l'AGP d'ADRC.

6.2.7 Méthode d'activation de clés privées

L'entité doit être authentifiée au module de chiffrement avant l'activation de la clé privée. Cette authentification peut se présenter sous forme de mot de passe. En cas de désactivation des clés, celles-ci doivent être conservées sous leur forme chiffrée seulement.

6.2.8 Méthode de désactivation de clés privées

Quand les clés sont désactivées, elles doivent être supprimées de la mémoire avant désattribution de celle-ci. Tout espace disque dans lequel étaient conservées les clés doit être écrasé avant la libération de celui-ci au système d'exploitation. Le module de chiffrement doit automatiquement désactiver la clé privée après une période prédéterminée d'inactivité.

6.2.9 Méthode de destruction de clés privées

À la fin de l'emploi d'une clé privée, toutes les copies de celle-ci dans la mémoire informatique et dans l'espace disque partagé doivent être détruites de façon sécuritaire par écrasement. La méthode d'écrasement doit être approuvée par l'AGP d'ADRC. Les procédures de destructions de clés privées doivent être décrites dans l'ÉPC ou dans tout autre document disponible publiquement.

6.3 Autres aspects de la gestion de paires de clés

6.3.1 Archivage des clés publiques

Sans objet.

6.3.2 Périodes d'emploi des clés publiques et privées

Les clés de 1024 bits doivent comporter des périodes de validité d'au plus deux ans.

Les clés de 2048 bits doivent comporter des périodes de validité d'au plus vingt ans.

Période de validité suggérée (1024) :

- Clé de vérification publique et certificat de l'AC – deux ans;
- Clé privée de signature de l'AC – un an;
- Clé de vérification publique et certificat de l'entité finale – un an;
- Clé privée de signature de l'entité – six mois.

Période de validité suggérée (2048) :

- Clé de vérification publique et certificat de l'AC – vingt ans;
- Clé privée de signature de l'AC – huit ans;
- Clé de vérification publique et certificat de l'entité finale – douze ans;
- Clé privée de signature de l'entité – deux ans.

L'emploi de longueurs de clés particulières devrait être déterminé conformément aux évaluations de la menace et des risques d'ADRC.

6.4 Données d'activation

6.4.1 Production et installation des données d'activation

Toute donnée d'activation doit être unique et imprévisible. Les données d'activation, de pair avec tout autre contrôle d'accès. doit comporter un niveau de résistance approprié pour les clés ou les données à protéger. En cas d'emploi d'un mot de passe, une entité doit avoir la capacité de modifier en tout temps celui-ci.

6.4.2 Protection des données d'activation

Les données utilisées pour l'initialisation de l'entité finale doivent être protégées de tout usage non autorisé à l'aide d'une combinaison de mécanismes de contrôle d'accès matériel et de chiffrement.

6.4.3 Autres aspects des données d'activation

Aucune disposition.

6.5 Contrôles de sécurité informatiques

6.5.1 Exigences techniques précises en matière de sécurité informatique

Les serveurs de l'AC doivent comprendre la fonctionnalité suivante :

- contrôle d'accès aux services de l'AC et aux rôles de l'ICP;
- séparation obligatoire des tâches pour les rôles de l'ICP;
- identification et authentification des rôles de l'ICP et des identités connexes;
- réutilisation ou séparation d'objets pour la mémoire à accès aléatoire de l'AC;
- emploi du chiffrement pour la communication entre séances et la sécurité des bases de données;
- archivage des données historiques et de vérification de l'entité finale et de l'AC;
- vérification des événements liés à la sécurité;
- autoessai des services d'AC liés à la sécurité;
- chemin de communications de confiance pour l'identification des rôles de l'ICP et des identités connexes;
- mécanismes de récupération pour les clés et le système de l'AC.

Cette fonctionnalité peut être assurée par le système d'exploitation ou par une combinaison du système d'exploitation, des logiciels de l'AC pour l'ICP et des dispositifs de protection matériels.

6.5.2 Classement de la sécurité informatique

Classement de la sécurité informatique (niveau d'évaluation CC) - À déterminer.
Le CST, la NSA ou tout autre laboratoire accrédité d'une tierce partie doit évaluer les éléments critiques en matière de sécurité de l'AC. Une telle évaluation doit comprendre l'analyse au niveau du système.

6.6 Contrôles techniques du cycle de vie

6.6.1 Contrôles du développement de systèmes

L'AC doit utiliser les logiciels de l'AC qui ont été conçus et élaborés dans le cadre d'une méthodologie d'élaboration comme la MIL-STD-498, le System Security Engineering Capability Maturity Model (SSE CMM) ou le Information Systems Security Engineering Handbook.

La conception et l'élaboration doivent être appuyées par la vérification par une tierce partie de la conformité au processus et par des évaluations de la menace et des risques, afin d'influer sur la conception des mesures de protection de la sécurité et de minimiser le risque résiduel.

6.6.2 Contrôles de gestion de la sécurité

Une méthodologie officielle de gestion de la configuration doit être utilisée pour l'installation et la maintenance continue du système de l'AC. Les logiciels de l'AC, quand ils sont chargés pour la première fois, doivent fournir une méthode pour l'AC de vérifier si les logiciels du système :

- émanent du développeur de logiciels;
- n'ont pas été modifiés avant l'installation; et
- constituent la version voulue aux fins d'emploi.

L'AC doit fournir un mécanisme de vérification périodique de l'intégrité des logiciels.

L'AC doit également disposer de mécanismes et de politiques pour le contrôle et la surveillance de la configuration du système de l'AC.

À l'installation, et au moins une fois par semaine, l'intégrité du système de l'AC doit être validé.

6.7 Contrôles de sécurité de réseau

Le serveur de l'AC doit être protégé contre toute attaque par un réseau ouvert ou polyvalent auquel il est raccordé. Une telle protection doit être fournie par l'installation d'un dispositif configuré afin de permettre uniquement les protocoles et commandes nécessaires à l'exploitation de l'AC.

L'AC doit s'assurer que son ÉPC définit les protocoles et commandes nécessaires aux fins de l'exploitation de l'AC.

6.8 Contrôles de conception du module de chiffrement

Toutes les activités de production de clés de signature numérique de l'AC, de stockage de clés de signature numérique de l'AC et de signature de certificats doivent être exercées dans un module de chiffrement matériel coté au moins au niveau 2 de la PUB FIPS 140-1 ou être vérifiées autrement à un niveau de fonctionnalité et d'assurance équivalent. Toutes les autres activités de chiffrement de l'AC doivent être exercées dans un module de chiffrement validé au moins au niveau 2 de la PUB FIPS 140-1 ou être vérifiées autrement à un niveau de fonctionnalité équivalent.

Les activités de production et de signature des clés de signature numérique de l'administrateur de l'ALE doivent être exercées dans un module de chiffrement matériel coté au moins au niveau 1 de la PUB FIPS 140-1 ou être vérifiées autrement à un niveau de fonctionnalité et d'assurance équivalent.

Toutes les autres activités de chiffrement de l'ALE doivent être exercées dans des modules de chiffrement cotés au niveau 1 de la PUB FIPS 140-1 ou être vérifiées autrement à un niveau de fonctionnalité et d'assurance équivalent.

Les entités finales doivent utiliser les modules de chiffrement validés au moins au niveau 1 de la PUB FIPS 140-1 ou être vérifiées autrement à un niveau de fonctionnalité et d'assurance équivalent.

7. Profils des certificats et des LCR

7.1 Profil des certificats

7.1.1 Numéro de version

L'AC doit délivrer les certificats X.509 de version 3, conformément au profil de certificats et de LCR de l'ICPX.

Les logiciels de l'entité finale de l'ICP doivent appuyez tous les champs de base (sans extension) X.509 :

- **Signature**: signature de l'AC pour authentifier le certificat
- **Issuer**: nom de l'AC
- **Validity**: date d'activation et d'expiration pour le certificat
- **Subject**: nom distinctif de l'abonné
- **Subject Public Key Information**: ID, clé de l'algorithme
- **Version**: version du certificat X.509, version 3(2)
- **Serial Number**: numéro de série unique pour le certificat

ainsi que les extensions du certificat définies à l'alinéa 7.1.2.

7.1.2 Extensions des certificats

Tous les logiciels d'ICP de l'entité traitent correctement les extensions désignées aux alinéas 4.2.1 et 4.2.2 du profil de certificat de l'ICPX. L'ÉPC doit définir l'emploi de toute extension appuyée par l'AC, ses ALE et les entités finales.

Le champ **certificatePolicies** doit être défini comme critique dans tous les certificats d'ICP d'ADRC.

7.1.3 ID d'objet d'algorithmes, points de distribution des LCR pour les divers niveaux d'assurance

L'AC doit utiliser et les entités finales doivent appuyer, pour la signature et la vérification, les algorithmes suivants :

- RSA 1024 ou 2048 conformément à PKCS#1 -[IDO à déterminer];
- SHA-1 conformément à la PUB FIPS 180-1 et à ANSI X9.30 (Partie 2) - [ID sha1WithRSAEncryption, IDO 1 2 840 113549 1 1 5, autorité de délivrance RSADSI].

Les entités peuvent utiliser, pour la signature et la vérification, les algorithmes suivants :

- RSA 1024, RSA 2048 conformément à PKCS#1 - [IDO à déterminer];
- DSA conformément à DSS (PUB FIPS 186) et à ANSI X9.30 (Partie 1) - [IDO à déterminer];
- MD5 conformément à ADC 1321 - [IDO à déterminer];
- SHA-1 conformément à la PUB FIPS 180-1 et à ANSI X9.30 (Partie 2) - [ID sha1WithRSAEncryption, IDO 1 2 840 113549 1 1 5, autorité de délivrance RSADSI].

7.1.4 Formes des noms

Chaque ND doit se présenter sous la forme d'une chaîne **printableString** X.501.

7.1.5 Contraintes des noms

Les ND **Subject** et **Issuer** doivent être conformes aux normes ICPX et être présentes dans tous les certificats.

7.1.6 Identificateur d'objet de la politique de certification

L'AC doit s'assurer que l'IDO de la politique est incluse dans les certificats qu'elle émet.

7.1.7 Emploi d'une extension de contraintes de politique

L'AC doit diffuser et marquer comme critique l'extension **policyConstraints**.

7.1.8 Syntaxe et sémantique des qualificateurs de politique

L'AC doit diffuser l'extension **policyQualifiers** avec l'URI de sa PC. Si l'AC diffuse l'extension userNotice, ce texte devrait être limité à celui décrit à l'alinéa 2.1.1.

7.1.9 Sémantique de traitement pour l'extension critique de la politique de certification

Les extensions critiques doivent être interprétées comme elles sont définies dans l'ICPX.

7.2 Profil des LCR

7.2.1 Numéro de version

L'AC doit délivrer les LCR X.509 de version deux (2) conformément au profil des certificats et des LCR.

7.2.2 Extensions des LCR et des entrées de LCR

Tous les logiciels d'ICP de l'entité doivent traiter correctement toutes les extensions LCR désignées dans le profil des certificats et des LCR de l'ICPX. L'ÉPC doit définir l'emploi de toute extension appuyée par l'AC, pas ses ALE et par les entités finales.

8. Administration des spécifications

8.1 Procédures de modification des spécifications

8.1.1 Éléments pouvant changer sans avis

Aucun.

8.1.2 Modifications avec avis

Avant d'apporter des modifications à la présente politique de certification, l'AGP d'ADRC avisera l'ICC et les AC qui sont directement cocertifiées avec l'AC d'ADRC.

8.1.2.1 Liste d'éléments

Tous les éléments de la présente politique de certification sont sujets à l'exigence relative aux avis.

8.1.2.2 Mécanisme d'avis

L'AGP d'ADRC avisera par écrit toutes les AC qui sont directement cocertifiées avec l'AC d'ADRC de toute modification proposée à la présente politique de certification. L'avis doit renfermer un énoncé des modifications proposées, la date finale de réception des commentaires et la date de modification proposée en vigueur. L'AGP d'ADRC doit demander aux AC d'aviser les abonnés de toutes les modifications proposées. L'AGP d'ADRC affichera également un avis de la proposition sur le site Web de l'AGP d'ADRC.

8.1.2.3 Période de commentaires

La période de commentaires sera de 30 jours, à moins d'avis contraire. La période de commentaires sera définie dans l'avis.

8.1.2.4 Mécanisme de traitement de commentaires

Les commentaires rédigés et signés relatifs aux modifications proposées doivent être adressés à l'AGP d'ADRC. Les décisions relatives aux modifications proposées sont à la discrétion de l'AGP d'ADRC.

8.1.2.5 Période pour l'avis de modifications final

L'AGP d'ADRC déterminera la période pour les avis de modifications finals.

8.1.2.6 Éléments dont les modifications exigent une nouvelle politique

Si, de l'avis de l'AGP d'ADRC, une modification à la politique exige la délivrance d'une nouvelle politique, l'AGP d'ADRC peut attribuer un nouvel identificateur d'objet (IDO) pour la politique modifiée.

8.2 Procédures de publication et d'avis

Une copie électronique du présent document, signée de façon numérique par un représentant autorisé de l'AC, doit être rendue disponible :

- sur le site Web de l'ICP de l'ADRC, https://reg-pki-ext.ccra-adrc.gc.ca/pki/welcome-f.html;
- par courriel à pkiadminicp@ccra-adrc.gc.ca

8.3 Procédures d'approbation des ÉPC

L'accréditation de l'AC doit être conforme aux procédures énoncées par l'AGP d'ADRC. Si un ÉPC renferme des renseignements relatifs à la sécurité de l'AC, il n'est pas nécessaire que les renseignements de l'ÉPC, en tout ou en partie, soient rendus publics.