Centre d'analyse des opérations et déclarations financières du Canada (CANAFE)

Politiques de certification

Déclaration externe - Confidentialité
Déclaration externe - Signature numérique

Version 1.0

Le 10 mai 2002

TABLE DES MATIÈRES

1. INTRODUCTION

1.1 Aperçu

Le présent document définit les politiques de certification (PC) suivantes concernant la délivrance de certificats de signature numérique et de confidentialité devant servir aux déclarations électroniques transmises à CANAFE :

- Politique de certification relative à la signature numérique aux fins de la déclaration externe
- Politique de certification relative à la confidentialité aux fins de la déclaration externe

Les certificats délivrés conformément aux présentes politiques de certification doivent servir exclusivement aux échanges avec CANAFE et constituent des « certificats d'entreprise ». Ils lient de manière sûre leur détenteur à ses clés publiques et sont gérés dans le cadre d'une Infrastructure à clé publique (ICP).

Les navigateurs standard du commerce prennent en charge les « certificats Web » mais non les certificats d'entreprise. L'autorité de certification (AC) régie par les présentes politiques de certification ne prend pas en charge, quant à elle, les certificats Web.

La politique de certification relative à la signature numérique aux fins de la déclaration externe a trait à la gestion et à l'emploi de certificats renfermant des clés publiques utilisées pour l'authentification et l'intégrité des données.

La politique de certification relative à la confidentialité aux fins de la déclaration externe a trait à la gestion et à l'emploi de certificats renfermant des clés publiques utilisées pour l'établissement de clés de chiffrement, y compris le transfert de clés. Les certificats délivrés dans le cadre de cette politique servent notamment à protéger des renseignements.

À moins que ces certificats soient utilisés de pair avec d'autres mécanismes de sécurité, ils ne doivent pas servir à protéger des renseignements dont l'atteinte à l'intégrité pourrait entraîner un préjudice grave dans le cas d'un intérêt non national ou des renseignements classifiés. Ces certificats ne doivent pas être utilisés là où la loi l'interdit ou en présence d'applications fonctionnant en mode dégradé.

CANAFE décline toute responsabilité de quelque nature que ce soit, découlant d'un délit, d'un contrat ou de toute autre forme de réclamation en ce qui a trait à l'emploi, à la délivrance, à l'octroi d'une licence ou à la fiabilité de certificats délivrés conformément aux présentes politiques de certification ou de paires afférentes de clés publiques/privées pour tout emploi autre que celui conforme aux présentes politiques de certification et à toute autre entente connexe.

La disponibilité des services qu'offre l'AC pourra être affectée par la maintenance du système ou par des facteurs hors du contrôle de l'AC. CANAFE décline toute responsabilité de quelque nature que ce soit pour des questions qui ne sont pas de son ressort, y compris la disponibilité ou la possibilité d'exploiter Internet ou des systèmes de télécommunications ou d'autres liés à l'infrastructure. Le terme « assurance » dans le présent document ne vise pas à émettre la représentation ou la garantie que de tels services soient disponibles.

1.2 Identification des politiques

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Le nom de cette politique est Politique de certification de CANAFE relative à la signature numérique de l'ICP aux fins de la déclaration externe. La désignation d'identificateur d'objet (IDO) alphanumérique et numérique de cette politique est : 2.16.124.101.1.275.2	Le nom de cette politique est Politique de certification de CANAFE relative à la confidentialité de l'ICP aux fins de la déclaration externe. La désignation d'identificateur d'objet (IDO) alphanumérique et numérique de cette politique est : 2.16.124.101.1.275.1

1.3 Participants à l'ICP

Les présentes politiques de certification prennent en charge un groupe ICP défini dans les sous-sections qui suivent.

1.3.1 Autorité de certification

Toutes les mentions à l'autorité de certification (AC) font référence à l'AC de CANAFE, à moins d'avis contraire.

L'AC peut retenir les services d'une tierce partie pour assumer les responsabilités qui lui sont confiées dans le cadre des présentes politiques de certification.

L'AC doit rendre compte à l'autorité de gestion des politiques de CANAFE sur les sujets suivants :

a) Mise en pratique des politiques de certification choisies ou définies par l'autorité de gestion des politiques de CANAFE;

b) Élaboration d'un Énoncé de pratiques de certification (ÉPC) conformément aux présentes politiques de certification, afin de documenter la conformité de l'AC à ces politiques et à d'autres exigences;

c) Maintenance de l'ÉPC afin d'en assurer la tenue à jour suivant les besoins;

d) Supervision du personnel de l'AC accomplissant les fonctions d'AC conformément à l'ÉPC.

En ce qui concerne le fonctionnement concret des serveurs de l'AC, on notera les rôles importants suivants :

1) Un utilisateur maître de l'ICP qui est responsable de la configuration et de la maintenance du matériel et des logiciels pour le système de l'AC, du début et de la fin de la prestation des services de l'AC ainsi que de la création initiale des comptes pour les agents de l'ICP.
2) Un agent de l'ICP qui est responsable de la gestion des administrateurs de l'ICP ainsi que d'autres agents de l'ICP et de la configuration des politiques en matière de sécurité de l'AC.
3) Un administrateur de l'ICP qui est responsable de la gestion du processus d'initialisation des abonnés; de la création, du renouvellement ou de la révocation des certificats et de la distribution des jetons (suivant les besoins).

Le personnel de l'AC ne devrait pas vérifier ses propres activités.

Un centre d'aide de l'ICP est associé à l'AC; il est responsable d'offrir de l'assistance aux abonnés et aux détenteurs de certificats désignés relativement à la délivrance, à la tenue à jour ou à la révocation de certificats.

1.3.2 Autorités d'enregistrement

Une autorité d'enregistrement (AE) est une personne ou un organisme agissant au nom de l'AC; elle est responsable de vérifier l'identité d'un abonné ou, dans le cas d'un organisme client, d'un détenteur de certificat désigné. Au besoin, l'AE peut vérifier l'autorité d'un détenteur de certificat désigné agissant au nom d'un organisme client. Malgré que l'AE lance le processus donnant lieu à la délivrance de certificats de la part de l'AC, elle ne signe ni n'émet de certificats. L'AE peut recourir à un système dans lequel le processus d'identification est automatisé grâce à des secrets partagés et peut accomplir d'autres tâches que pourrait lui demander l'AC.

1.3.3 Abonnés

Les groupes suivants peuvent être des abonnés de l'AC :

1) Des personnes agissant en leur nom propre;
2) Des organismes de l'extérieur de CANAFE sous toutes les formes reconnues par la loi.

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

Les certificats régis par les présentes politiques de certification peuvent être délivrés aux employés de CANAFE, à des rôles, à des dispositifs ou à des applications, afin de faciliter la prestation de programmes. Cependant, ceux-ci ne constituent pas des abonnés au sens des présentes politiques de certification et d'autres instruments régiront leurs droits, privilèges et obligations.

1.3.4 Organismes clients

Comme il a été noté, un organisme de l'extérieur de CANAFE représente une forme d'abonné. Ces organismes peuvent souhaiter obtenir des certificats dont se serviront leurs employés et, à l'occasion et suivant les besoins, d'autres personnes qui sont autorisées à agir en leur nom. Ces personnes sont considérées comme des détenteurs de certificats désignés et détiennent les certificats délivrés dont se servent les personnes, les dispositifs, les rôles ou les applications de l'organisme client.

Les certificats devant servir au sein d'un organisme client seront délivrés sur demande seulement de la part d'une personne désignée par l'organisme comme étant la personne responsable chez le client (PRC) et qui est autorisée à déposer une telle demande.

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

1.3.5 Parties utilisatrices

Une partie utilisatrice peut être :

a) Un abonné de l'AC de CANAFE;

b) Une personne qui est un employé de CANAFE ou un entrepreneur autorisé; ou

c) Un dispositif ou une application sous le contrôle de CANAFE

qui utilise un certificat délivré dans le cadre des présentes politiques de certification et signé par l'AC, afin d'authentifier une signature numérique ou de chiffrer les communications destinées à un détenteur de certificat.

Les personnes ou les organismes autres que ceux énumérés ci-dessus ne sont pas autorisées à utiliser les certificats que délivre l'AC. S'ils les utilisent, ils le font à leur propre risque. CANAFE décline absolument toute responsabilité pouvant découler d'une telle utilisation.

1.3.6 Autres participants

Autorité de gestion des politiques de CANAFE

L'autorité de gestion des politiques de CANAFE est un comité interne composé des hauts dirigeants de CANAFE. Elle est responsable des aspects suivants :

a) Approbation des politiques de certification de l'AC de CANAFE;

b) Approbation de l'Énoncé des pratiques de certification de l'AC de CANAFE;

c) Orientation des politiques auprès de l'AC de CANAFE.

Gestionnaire de dépôt

Le gestionnaire de dépôt est une personne ou un organisme qui est responsable de la tenue à jour d'un dépôt de renseignements pertinents comme les certificats et les Listes des certificats révoqués (LCR).

L'AC disposera d'au moins un certificat et d'une LCR.

L'AC peut accomplir cette fonction mais n'en est pas obligée. Lorsqu'un dépôt n'est pas sous le contrôle de l'AC, celle-ci établira les conditions de son association avec le gestionnaire de dépôt. Ces conditions portent notamment sur la disponibilité, sur le contrôle d'accès, sur l'intégrité des données, sur la protection des renseignements personnels ainsi que sur la reproduction et le chaînage des répertoires.

1.4 Emploi des certificats

1.4.1 Emplois convenables des certificats

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Cette politique convient à l'intégrité et à l'authentification des opérations ou des communications.	Cette politique convient à la protection des renseignements.

1.4.2 Emplois interdits des certificats

Les certificats délivrés par l'AC ne doivent pas servir dans les cas suivants :

1) Toute application devant fonctionner en mode dégradé;

2) Les opérations dans lesquelles la réglementation applicable interdit l'emploi de signatures numériques ou qui sont interdites par la loi; ou

3) À moins que d'autres mécanismes de sécurité convenables n'en assurent la prise en charge, la protection de :

    i) renseignements dont l'atteinte à l'intégrité pourrait entraîner un préjudice grave dans le cas d'un intérêt non national; ou

    ii) renseignements classifiés.

1.5 Administration des politiques

1.5.1 Organisme responsable des présentes politiques de certification

L'autorité de gestion des politiques de CANAFE (AGP de CANAFE) est responsable des présentes politiques de certification.

1.5.2 Renseignements sur les contacts

Président, Autorité de gestion des politiques de CANAFE
CANAFE
Ottawa (Ontario) Canada
K1P 1H7
Télécopieur : (613) 943-7931
Courriel : icp@canafe.gc.ca

1.5.3 Avis et publication

L'AC :

a) Fournira aux abonnés, aux organismes clients, aux détenteurs de certificats désignés et aux parties utilisatrices l'adresse URL de son site Web;

b) Publiera sa PC sur son site Web;

c) Fera part aux abonnés, aux détenteurs de certificats désignés et aux parties utilisatrices de toute modification apportée au sujet de leurs droits, privilèges et obligations concernant les certificats;

d) Transmettra à sa discrétion aux parties pertinentes, selon les conditions qu'elle juge appropriées, tout ou partie de l'ÉPC, aux fins de vérification, d'inspection ou d'accréditation.

1.5.4 Modification aux politiques de certification

L'AGP de CANAFE peut modifier les présentes politiques de certification ou une partie de celles-ci, et ce en tout temps et à sa discrétion.

1.5.5 Approbation de l'Énoncé de pratiques de certification

Après qu'il est déterminé que l'ÉPC décrit de manière satisfaisante la façon dont l'AC mettra en pratique les exigences précisées dans les présentes politiques de certification, l'AGP de CANAFE l'approuvera selon ces politiques et les modifications qui y auront été apportées.

1.6 Définitions et acronymes

1.6.1 Définitions générales

Abonné	Personne ou organisme dont les certificats à clé publique sont signés par l'AC régie par les présentes politiques de certification.
Administrateur de l'ICP	Personne responsable de la gestion du processus d'initialisation des abonnés ainsi que de la création, du renouvellement ou de la révocation des certificats et de la distribution des jetons (suivant les besoins).
Agent de l'ICP	Personne responsable de la gestion des administrateurs de l'ICP ainsi que d'autres agents de l'ICP et de la configuration des politiques en matière de sécurité de l'AC.
Autorité de certification	Autorité en qui une ou plusieurs entités finales mettent leur confiance pour délivrer et gérer les LCR et les certificats à clé publique conformes X.509. L'AC doit rendre compte à l'autorité de gestion des politiques sur les sujets suivants : a) Mise en pratique des politiques de certification choisies ou définies par l'autorité de gestion des politiques; b) Élaboration d'un Énoncé de pratiques de certification (ÉPC) conformément aux présentes politiques de certification, afin de documenter la conformité de l'AC à ces politiques et à d'autres exigences; c) Maintenance de l'ÉPC afin d'en assurer la tenue à jour suivant les besoins; d) Supervision du personnel de l'AC accomplissant les fonctions d'AC conformément à l'ÉPC.
Autorité de gestion des politiques de CANAFE	L'autorité de gestion des politiques de CANAFE est un comité interne composé des hauts dirigeants de CANAFE. Elle est responsable des aspects suivants : a) Approbation des politiques de certification de l'AC de CANAFE; b) Approbation de l'Énoncé des pratiques de certification de l'AC de CANAFE; c) Orientation des politiques auprès de l'AC de CANAFE.
Autorité de gestion des politiques du GC	L'autorité de gestion des politiques du gouvernement du Canada est un comité interministériel composé de hauts dirigeants du GC. Elle est responsable des aspects suivants : a) Approbation des politiques de certification de l'AC du GED; b) Approbation de l'Énoncé de pratiques de certification de l'AC du GED; c) Orientation des politiques auprès de l'AC du GED; d) Recommandation de toute cocertification ou de toute entente sur la possibilité d'interfonctionnement avec les domaines des AC

	externes. L'autorité de gestion des politiques rend compte au Secrétariat du Conseil du Trésor de l'orientation et de la gestion de l'infrastructure à clé publique du gouvernement du Canada.
Autorité d'enregistrement	Personne ou organisme responsable de l'identification et de l'authentification des abonnés et d'autres entités finales avant la délivrance des certificats, mais qui ne signe ni n'émet ceux-ci. Il est possible qu'une AE doive accomplir certaines tâches au nom de l'AC.
Autorité d'état des certificats	Entité en qui l'on met sa confiance pour vérifier en ligne la validité du certificat d'une partie utilisatrice et qui peut également fournir des renseignements supplémentaires au sujet des caractéristiques d'un certificat.
Certificat	Fichier électronique de format conforme à la Recommandation UIT-T X.509 renfermant la clé publique d'un abonné ou d'un détenteur de certificat désigné, accompagnée des renseignements connexes et signée de façon numérique avec la clé privée de l'autorité de certification qui l'a délivrée.
Certificat d'entreprise	Certificat délivré par une AC et devant servir à des personnes, à des organismes, à des rôles, à des dispositifs ou à des applications. Ces certificats sont entièrement gérés dans une ICP et peuvent être soumis aux éléments suivants : a) Vérification automatique de la révocation; b) Mise à jour transparente des pièces d'identité; c) Mise à jour dynamique et transparente de la politique en matière de sécurité. Un certificat d'entreprise lie de manière sûre le propriétaire du certificat à ses clés publiques. Les navigateurs standard du commerce ne prennent pas en charge les certificats d'entreprise.
Certificat Web	Certificat délivré à des utilisateurs (p. ex. des clients et des serveurs) par une AC, qui lie de manière sûre le propriétaire du certificat à ses clés publiques. D'habitude, une clé racine pour l'AC est intégrée aux navigateurs du commerce, ce qui permet la vérification de sites Web.
Chaîne de validation de la certification	Chaîne de certificats débutant par le certificat d'un détenteur d'une clé publique (une entité) signé par une AC – le certificat de l'AC de l'entité - et un ou plusieurs autres certificats des AC signés par d'autres AC. Si l'utilisateur de la clé publique (partie utilisatrice) ne détient pas déjà une copie sécurisée de la clé publique de l'AC ayant signé le certificat de l'entité, le nom de l'AC et les renseignements connexes (comme la période de validité ou les contraintes liées au nom), il lui faudra peut-être recourir à un certificat supplémentaire pour obtenir la clé publique aux fins de vérification. Souvent, une chaîne composée de nombreux certificats peut être nécessaire. Ces chaînes s'appellent chemins de certification.
Cocertificat	Certificat délivré par une autorité de certification et servant à établir un lien de confiance entre deux autorités de certification.
Dépôt	Système de stockage des LCR, des LCAR et des certificats à clé publique aux fins d'accès par les entités. Un annuaire X.500 constitue un exemple de

	dépôt.
Détenteur de certificat désigné	Personne d'un organisme client qui est désignée comme détentrice d'un certificat délivré à une personne, à un rôle, à un dispositif ou à une application au sein de l'organisme client.
Données d'activation	Données privées (autres que des clés) nécessaires pour accéder à des environnements de sécurité personnelle qui doivent être protégés (p. ex. mot de passe).
Données d'initialisation	Codes ou autres données dont se sert un abonné ou un détenteur de certificat désigné pour produire une clé privée de signature numérique et pour obtenir des certificats à clé publique de la part de l'AC (p. ex. numéro de référence et code d'authentification).
Enregistrement	Processus par lequel une personne ou un organisme s'enregistre pour recevoir des services ou pour mener des opérations avec CANAFE.
Entité	Tout élément autonome dans l'ICP. Il peut s'agit d'une AC, d'une AE ou d'une entité finale.
Entité finale	Entité utilisant les clés et les certificats créés dans une infrastructure à clé publique pour des fins différentes de celles de la gestion des clés et des certificats. Une entité finale peut être un abonné, un détenteur de certificat désigné ou une partie utilisatrice ou encore un dispositif, un rôle ou une application qui utilise un certificat attribué à un détenteur de certificat désigné.
Environnement contrôlé	Combinaison de produits matériels et logiciels, d'outils de gestion de la configuration, de politiques et de procédures utilisés pour gérer les environnements d'abonnés ou de détenteurs de certificats désignés que contrôle un gestionnaire fonctionnel de programme et/ou l'organisme client. Si un organisme client contrôle principalement l'environnement, le rapport fonctionnel existant entre le programme et l'organisme client peut comporter des obligations en matière de sécurité, et ce pour toute entente liée au programme, afin de réduire au minimum les risques en matière de sécurité.
Environnement de sécurité personnelle	Zone de stockage sécurisée renfermant des renseignements comme les clés privées et les certificats connexes. Cette zone est chiffrée et protégée à l'aide du chiffrement. La forme de stockage peut varier de simples fichiers à des jetons de chiffrement infalsifiables.
Gestion de la configuration	Processus visant à déceler et à définir les points critiques d'un système et à contrôler toute modification apportée à ces points lors de leur cycle de vie.
Gestionnaire de dépôt	Personne ou organisme responsable de la tenue à jour d'un dépôt de renseignements pertinents comme les certificats et les Listes des certificats révoqués.
Identificateur d'objet	Identificateur alphanumérique/numérique unique enregistré conformément à la norme d'enregistrement ISO pour faire référence à un objet ou à une catégorie d'objet précise.
Infrastructure à clé publique	Ensemble des politiques, des processus, des plates-formes de serveurs, des logiciels et des postes de travail servant à la gestion des certificats et des clés.
Installation centrale	Autorité de certification de la passerelle ICP du gouvernement du Canada. Sous la supervision de l'autorité de gestion des politiques pour l'ICP du GC,

canadienne	l'ICC signe et gère les cocertificats des AC de haut niveau du GC et les AC autres que celles du GC. L'ICC ne gère pas les certificats des abonnés.
Intégrité des données	Lors de l'utilisation de signatures numériques, assurance que les données n'ont pas été modifiées depuis l'instant où une signature numérique a été appliquée aux données. Il existe d'autres moyens d'assurer l'intégrité des données, comme l'emploi de codes d'authentification de messages.
Liste des certificats de l'autorité révoqués	Liste des certificats de l'AC révoqués. Une LCAR constitue une Liste des certificats révoqués pour les cocertificats ou les certificats autosignés de l'AC.
Liste des certificats révoqués	Liste émise et conservée par l'autorité de certification des certificats qui sont révoqués avant leur expiration naturelle.
Logiciel d'autorité de certification	Logiciel de gestion de la clé de signature de l'AC, du cycle de vie des certificats et des LCR ainsi que des paires de clés des entités finales.
Ministère ou agence	Toute entité définie à l'Annexe I, Parties I.1 et II de la Loi sur la gestion des finances publiques (LGFP) (a) Toute commission qui, en vertu de la Loi sur les enquêtes, est désignée par ordre du gouverneur en conseil comme ministère aux fins de la LGFP; (b) Forces canadiennes; (c) Agences ou sociétés d'État qui ont passé des ententes ou ont convenu de dispositions avec le Secrétariat du Conseil du Trésor pour adopter les exigences des présentes politiques de certification et pour les appliquer à leur organisme.
Mode dégradé	Conception de la structure de programmes et/ou de systèmes de traitement de façon à assurer la sécurité et/ou à accomplir les missions qui leur sont confiées en cas de détection d'une panne matérielle ou logicielle dans un programme ou un système.
Mode sûr	Conception de la structure de programmes et/ou de systèmes de traitement de façon à empêcher l'introduction de vulnérabilités liées à la sécurité en cas de détection d'une panne matérielle ou logicielle dans un programme ou un système.
Non-répudiation	Dans un contexte juridique, le terme « non-répudiation » signifie qu'il y a une preuve suffisante pour convaincre un arbitre quant à l'origine et à l'intégrité des données signées par voie numérique, malgré une tentative de déni de la part du prétendu expéditeur. Dans un contexte technique, le terme « non-répudiation » signifie que la partie utilisatrice a l'assurance que si une clé publique de vérification a été utilisée pour valider une signature numérique, cette signature doit avoir été faite par la clé privée de signature correspondante.

Organisme	Agence, société, partenariat, fiducie, coentreprise ou toute autre association. S'il est reconnu comme tel, un organisme peut comprendre une entreprise à propriétaire unique.
Organisme client	Organisme constituant un client ou une entité de déclaration de CANAFE.
Partie utilisatrice	Entité qui est : a) Un abonné de l'AC de CANAFE; b) Une personne qui est un employé de CANAFE ou un entrepreneur autorisé; ou c) Un dispositif ou une application sous le contrôle de CANAFE qui utilise un certificat délivré dans le cadre des présentes politiques de certification et signé par l'AC, afin d'authentifier une signature numérique ou de chiffrer les communications destinées à un détenteur de certificat.
Personne morale	Personne naturelle distinguée d'un groupe ou d'une catégorie ou de tout type d'organisme.
Personne responsable chez le client	Personne d'un organisme client qui est autorisée à le représenter et à agir en son nom pour déposer des demandes de délivrance de certificats. D'habitude, une personne responsable chez le client est responsable des aspects suivants : a) Vérification et confirmation de l'identité et des pièces justificatives des détenteurs de certificats désignés au sein d'un organisme client; b) Communication à l'AC de tout changement des rapports qu'entretient l'organisme client avec un détenteur de certificat désigné ou des renseignements qu'elle lui fournit, ce qui aurait comme résultat de mettre fin au certificat ou d'en faire la mise à jour.
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 transformation a été créée à l'aide de la clé correspondant à celle du signataire; b) si les données ont été modifiées depuis la transformation.
Stockage	Processus au cours duquel les clés privées de signature et les clés privées de confidentialité sont stockées dans un profil situé sur un serveur exploité par l'AC. Lorsque les abonnés ou les détenteurs de certificats désignés souhaitent utiliser leurs clés, ils accèdent à leur profil à l'aide d'un ID d'utilisateur et d'un mot de passe précis qu'eux seuls connaissent et ils récupèrent le profil chiffré grâce à un tunnel SSL. Une fois la copie locale utilisée, celle-ci est détruite. Le profil n'est en aucun moment hors du contrôle exclusif de l'abonné ou du détenteur de certificat désigné.
Utilisateur maître de l'ICP	Personne responsable de la configuration et de la maintenance du matériel et des logiciels pour le système de l'AC, du début et de la fin de la prestation des services de l'AC ainsi que de la création initiale des comptes pour les agents de l'ICP.
Zone de sécurité	Secteur dans lequel l'accès est limité au personnel autorisé et aux visiteurs autorisés et escortés de façon appropriée. 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.

1.6.2 Acronymes

AC	Autorité de certification
AE	Autorité d'enregistrement
AGP	Autorité de gestion des politiques
CST	Centre de la sécurité des télécommunications
DCD	Détenteur de certificat désigné
DES	Data Encryption Standard
ÉMR	Évaluation de la menace et des risques
ÉPC	Énoncé de pratiques de certification
ESP	Environnement de sécurité personnelle
FIPS	Federal Information Processing Standards
GC	Gouvernement du Canada
GED	Gouvernement du Canada en direct
GFP	Gestionnaire fonctionnel de programme
I et A	Identification et authentification
ICC	Installation centrale canadienne
ICP	Infrastructure à clé publique
IDO	Identificateur d'objet
LCAR	Liste des certificats de l'autorité révoqués
LRC	Liste des certificats révoqués
ND	Nom distinctif
NDR	Nom distinctif relatif
OC	Organisme client
OCSP	Online Certificate Status Protocol
PC	Politique de certification
PRC	Personne responsable chez le client
RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Algorithm -1
SSL	Secure Sockets Layer
UIT	Union internationale des télécommunications
URL	Localisateur de ressources uniforme

2. DISPOSITIONS GÉNÉRALES, LÉGALES ET COMMERCIALES

2.1 Représentations et garanties

2.1.1 Représentations et garanties de l'AC

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
L'AC est responsable des aspects suivants : a) Création et signature des certificats liant les abonnés, les détenteurs de certificats désignés, le personnel de l'ICP et (si cela est permis) d'autres AC à leurs clés publiques de vérification; b) Promulguer l'état des certificats grâce aux LCR. L'AC peut également produire des paires de clés de signature numérique pour des entités finales lorsqu'elle utilise les processus d'enregistrement automatisés.	L'AC est responsable des aspects suivants : a) Création et signature des certificats liant les abonnés, les détenteurs de certificats désignés et le personnel de l'ICP à leurs clés publiques de chiffrement; b) Promulguer l'état des certificats grâce aux LCR. L'AC produira également des paires de clés de confidentialité pour des entités finales, suivant les besoins.

L'AC doit :

1) Servir aux fins de délivrance et de gestion des certificats pour les abonnés, les détenteurs de certificats désignés, le personnel de l'AC, les AE et les gestionnaires de dépôts, suivant les besoins, conformément aux présentes politiques de certification, l'ÉPC pertinent et les lois pertinentes du Canada;
2) Préparer un ÉPC décrivant en détails toutes les pratiques, les procédures et les exigences nécessaires pour assurer la conformité aux présentes politiques de certification;
3) S'assurer que toutes les AE et que tous les gestionnaires de dépôts agissant en son nom agissent conformément aux présentes politiques de certification et à l'ÉPC pertinent;
4) S'assurer que des ententes convenables décrivant les grandes lignes des droits, des privilèges et des obligations respectifs des parties sont intervenues entre les groupes suivants :
    a) Les abonnés pour les certificats qui leur sont délivrés ou dont la direction leur est confiée;
    b) Toutes les autres personnes qui accomplissent des fonctions au nom de l'AC.
5) Fournir, dans un document rendu public, des renseignements comme ceux précisant que les demandeurs peuvent demander la délivrance d'un certificat, sa suspension ou sa révocation;
6) Agir afin de fournir aux abonnés, aux personnes responsables chez le client et aux parties utilisatrices un avis concernant leurs droits, leurs privilèges et leurs obligations respectifs quant à l'emploi de clés d'ICP, de certificats, de matériel et de logiciels transmis par l'AC;
7) Aviser un abonné, une personne responsable chez le client ou un détenteur de certificat désigné, suivant le cas, lorsqu'un certificat à leur intention est :

a) Délivré;

b) Suspendu; ou

c) Révoqué.

8) S'assurer que le processus d'initialisation prend fin dans une période préétablie, comme il est documenté dans l'ÉPC;

9) Fournir un avis concernant l'adresse de la LCR dans les certificats délivrés dans le cadre des présentes politiques;

10) Fournir un avis convenable à toutes les parties intéressées quant aux procédures de l'AC concernant l'expiration, la suspension, la révocation et le renouvellement de certificats;

11) Mettre les LCR à la disposition d'un abonné, d'un détenteur de certificat désigné ou d'une partie utilisatrice, suivant les besoins, conformément aux présentes politiques de certification;

12) Utiliser sa clé privée de signature de certificats seulement pour signer les certificats et les LCR et pour aucune autre fin;

13) Instituer des procédures pour s'assurer que le personnel de l'AC associé aux rôles d'ICP (p. ex. utilisateur maître de l'ICP, agents de l'ICP et administrateurs de l'ICP) est responsable des gestes qu'il pose et pour s'assurer qu'une preuve permet de lier un geste à la personne qui le pose;

14) S'assurer que le personnel de l'AC utilise les clés privées qui lui ont été délivrées afin d'accomplir les tâches de l'AC, à ces seules fins.

Sauf indication contraire, la publication d'un certificat dans un dépôt constitue la certification de l'AC. Par ailleurs, l'avis transmis à un abonné ou à une partie utilisatrice qui peut accéder au certificat dans le dépôt signifie que les renseignements présentés dans le certificat ont été vérifiés et sont conformes aux présentes politiques de certification.

SIGNATURE NUMÉRIQUE	**CONFIDENTIALITÉ**
Suivant les besoins découlant de la technologie utilisée, l'AC disposera les clés privées de signature de l'abonné ou du détenteur de certificat désigné dans le stockage.	Suivant les besoins découlant de la technologie utilisée, l'AC disposera les clés privées de déchiffrement de l'abonné ou du détenteur de certificat désigné dans le stockage.

2.1.2 Représentations et garanties de l'AE

L'AE doit :

1) Se conformer aux dispositions pertinentes des présentes politiques de certification et de l'ÉPC et aux conditions de toute entente ou de toute disposition intervenue avec l'AC;

2) Transmettre aux demandeurs le processus de dépôt de demandes, y compris le processus d'initialisation de certificats;

3) Identifier et authentifier les demandeurs cherchant à devenir des abonnés et, lors de présentation des renseignements concernant les demandes à l'AC, certifier à l'AC qu'elle a procédé de manière conforme aux exigences des présentes politiques de certification;

4) Informer les abonnés, les personnes responsables chez le client ou les détenteurs de certificats désignés, le cas échéant, des aspects suivants :

i) Leurs droits, privilèges et obligations respectifs quant à l'emploi de clés d'ICP, de certificats, de matériel et de logiciels transmis par l'AC;

ii) Les procédures de l'AC concernant l'expiration, la suspension, la révocation et le renouvellement de clés et de certificats;

5) Si l'AC ne consigne pas ces renseignements, s'assurer, aux fins de vérification, de tenir à jour un registre des gestes posés pour l'accomplissement des tâches de l'AE.

6) Protéger les clés privées de l'AE, suivant les directives transmises par l'AC.

Les AE peuvent prendre en charge les processus d'enregistrement en ligne et hors ligne.

2.1.3 Représentations et garanties de l'abonné

Un abonné doit :

1) S'assurer que les renseignements présentés à l'AC ou à l'AE directement ou en leur nom sont complets et exacts;

2) Se conformer aux conditions de l'entente pertinente avec l'abonné ou à tout autre instrument de liaison que l'AC juge satisfaisant;

3) Utiliser les clés ou les certificats aux seules fins permises par les présentes politiques de certification et à aucune autre fin;

4) Mener les opérations de chiffrement voulues à l'aide des logiciels et du matériel convenables;

5) Protéger ses clés privées, ses mots de passe et ses jetons de clés (le cas échéant) de la manière définie dans les présentes politiques de certification ou suivant les directives et prendre toutes les mesures raisonnables pour empêcher la perte, la divulgation, la modification ou l'emploi non autorisé;

6) Assumer la responsabilité pour la protection de tout renseignement par suite de son déchiffrement et/ou de sa vérification, en particulier lorsque l'abonné choisit de rechiffrer les renseignements aux fins de stockage;

7) Aviser immédiatement l'AC de la manière précisée par l'AC, en cas d'atteinte à l'intégrité réelle ou soupçonnée des clés privées, du mot de passe ou des jetons de clés (le cas échéant) de l'abonné;

8) En ce qui concerne l'emploi, à l'extérieur du Canada, de matériel ou de logiciels renfermant des produits ou des éléments de chiffrement, vérifier les aspects suivants :

i) L'importation et/ou l'utilisation de tels produits est permise dans un pays ou une juridiction donnée;

ii) L'exportation de tels produits depuis le Canada vers un autre pays ou une autre juridiction est permise.

2.1.4 Représentations et garanties de l'organisme client

Lorsqu'un abonné constitue un organisme (« organisme client ») et dépose une demande afin de recevoir des certificats dont se serviront des personnes, des dispositifs, des applications ou des rôles (« détenteurs de certificats désignés »), l'organisme client, outre les exigences mentionnées à la section 2.1.3, doit également :

1) Assumer l'entière responsabilité liée à l'emploi des clés, des certificats, du matériel ou des logiciels délivrés aux détenteurs de certificats désignés par l'AC;

2) Nommer une ou plusieurs personnes autorisées à agir en son nom et en confirmer l'identité (« personne(s) responsable(s) chez le client »);

3) Par l'entremise de cette ou de ces personnes responsables chez le client, vérifier l'identité et les pièces d'identité des personnes qui doivent détenir les certificats pour leur propre emploi ou pour l'emploi de dispositifs, d'applications ou de rôles organisationnels au sein de l'organisme client, et communiquer ces renseignements à l'AC ou à une AE;
4) Certifier que tous les renseignements que doivent contenir de tels certificats et que toute demande de services de l'AC seront exacts et complets;
5) S'assurer que personne d'autre que le détenteur de certificat désigné aura accès aux clés privées de signature dont ils sont responsables;
6) S'assurer que toutes les données d'activation associées aux environnements de sécurité personnelle (ESP) pour de tels certificats demeurent confidentiels;
7) En ce qui concerne les certificats pour des dispositifs, des applications ou des rôles, s'assurer qu'une seule personne est responsable de ces certificats pour toute période donnée;
8) Aviser l'AC ou l'AE si le rapport entre l'organisme client et le détenteur de certificat désigné a changé de telle sorte que le certificat devrait être révoqué ou mis à jour ou si un changement a été apporté au sujet des renseignements sur le détenteur de certificat désigné ou de l'autorisation qu'il détient d'agir au nom de l'organisme client relativement aux déclarations à CANAFE;
9) Documenter, détenir et produire sur demande des dossiers sur l'état et l'autorisation des employés aux fins de vérification, ces dossiers devant lier une personne donnée à un certificat voulu pendant la période au cours de laquelle le certificat est confié au détenteur de certificat désigné;
10) S'assurer que les détenteurs de certificats désignés :
    i) Utilisent les clés ou les certificats aux seules fins permises par les présentes politiques de certification;
    ii) Mènent les opérations de chiffrement voulues à l'aide des logiciels et du matériel convenables;
    iii) Protègent les clés privées, les mots de passe et les jetons de clés (le cas échéant) qui leur sont confiées de la manière définie dans les présentes politiques de certification ou suivant les directives et prennent toutes les mesures raisonnables pour empêcher leur perte, leur divulgation, leur modification ou leur emploi non autorisé;
    iv) Avisent immédiatement l'AC de la manière précisée par l'AC, en cas d'atteinte à l'intégrité réelle ou soupçonnée des clés privées associées au certificat qu'il détient.

Les clés privées d'un abonné ou d'un détenteur de certificat désigné doivent être stockées de manière sûre dans un environnement de sécurité personnelle (ESP).

Un organisme client devrait :

a) Appliquer régulièrement des mécanismes anti-virus et les tenir à jour;
b) Appliquer les mises à jour de logiciels à des postes de travail clients;
c) Protéger les postes de travail clients à l'aide de services de pare-feu;
d) Maintenir la gestion de la configuration pour l'environnement client afin de réduire au minimum les vulnérabilités;
e) Maintenir une séparation nette des tâches entre les activités d'administration et de supervision (p. ex. vérifications) et les utilisateurs du système;
f) Mettre en place une politique de mot de passe selon laquelle, au minimum, (i) les valeurs implicites transmises par un fournisseur dans le cas de mots de passe de système sont modifiées immédiatement, (ii) les mots de passe transmis par un fournisseur ne sont pas

utilisés, (iii) les postes de travail clients, si cela est possible, présentent des comptes protégés par des mots de passe, (iv) les mots de passe, si cela est possible, se composent d'au moins 8 caractères avec une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.

2.1.5 Représentations et garanties de la partie utilisatrice

Une partie utilisatrice doit :

1) Mener les opérations de chiffrement voulues à l'aide des logiciels et du matériel convenables;
2) Avant de se fier à un certificat :
    i) Vérifier l'état du certificat par rapport aux LCR convenables et actuelles, conformément aux exigences énoncées à la section 4.4.10, suivant le cas;
    ii) En ce qui concerne la validation des certificats à l'aide d'une LCR, valider la signature numérique de l'AC apposée à la LCR.

2.1.6 Représentations et garanties du gestionnaire de dépôt

Lorsque l'AC exploite un dépôt ou autrement agit comme gestionnaire de dépôt, l'AC doit :

1) Publier les certificats et les LCR;
2) Informer les abonnés et les détenteurs de certificats désignés de l'emplacement de tout serveur de LCR;
3) Publier l'état des certificats grâce à la *Liste des certificats révoqués* ou autrement rendre les renseignements disponibles selon les échéances énoncées dans les présentes politiques de certification;
4) Configurer les contrôles d'accès au système d'exploitation et au dépôt, de sorte que seul le personnel autorisé de l'AC puisse écrire ou modifier la version en ligne de la PC.

Si l'AC n'exploite pas un dépôt, l'AC doit s'assurer par contrat ou par un autre moyen, que le gestionnaire de dépôt satisfait aux exigences précitées.

L'AC peut mandater les contrôles d'accès au dépôt en ce qui concerne les certificats, les LCR ou la vérification de l'état des certificats en ligne.

2.2 Dénis de garanties

CANAFE, ses employés, fonctionnaires ou agents ne font aucune représentation ni n'émettent aucune garantie ou condition, expresses ou implicites, autres que celles énoncées dans les présentes politiques de certification ou dans tout autre document autorisé à cette fin par CANAFE.

Aucun rapport de coentreprise, de partenariat, de société, d'organisme ou de fiducie n'est établi ni présumé être établi entre CANAFE et les personnes, les organismes ou autres utilisant les certificats délivrés par l'AC ou par une AC cocertifiée.

2.3 Limitations de responsabilité

CANAFE décline toute responsabilité de quelque nature que ce soit, découlant d'un délit, d'un contrat ou de toute autre forme de réclamation en ce qui a trait à l'emploi, à la délivrance, à l'octroi d'une licence ou à la fiabilité de certificats délivrés conformément aux présentes politiques de certification ou de paires de clés publiques/privées pour tout emploi autre que celui conforme aux présentes politiques de certification et à toute autre entente connexe.

CANAFE décline toute responsabilité de quelque nature que ce soit, découlant d'un délit, d'un contrat ou de toute autre forme de réclamation en ce qui a trait à l'exportation ou à l'importation de produits de chiffrement par des personnes ou des organismes.

La disponibilité des services qu'offre l'AC pourra être affectée par la maintenance du système ou par des facteurs hors du contrôle de l'AC. CANAFE décline toute responsabilité de quelque nature que ce soit pour des questions qui ne sont pas de son ressort, y compris la disponibilité ou la possibilité d'exploiter Internet ou des systèmes de télécommunications ou d'autres liés à l'infrastructure. Le terme « assurance » dans le présent document ne vise pas à émettre la représentation ou la garantie que de tels services soient disponibles.

Les dénis et limitations de responsabilité des présentes politiques de certification sont sujets à toute entente ou à toute disposition pouvant être intervenue par la Couronne aux droits du Canada et qui pourrait en décider autrement.

2.4 Cocertification et reconnaissance

Sans objet.

2.5 Protection des renseignements et des données

L'AC doit s'assurer que toute demande d'obtention d'un certificat à délivrer par l'AC renfermera des mentions voulant que le consentement du demandeur soit nécessaire pour la collecte, l'emploi et la divulgation de renseignements personnels, de la manière décrite dans les présentes politiques de certification et toute autre entente connexe.

2.5.1 Nature délicate des types de renseignements personnels

Les renseignements personnels constituent (1) des renseignements identifiables concernant une personne et (2) des renseignements confidentiels commerciaux concernant un organisme. La nature délicate des renseignements personnels que conserve CANAFE relativement aux certificats délivrés dans le cadre des présentes politiques de certification est déterminée en référence aux aspects suivants :

1) Les lois et règlements applicables, y compris notamment la *Loi sur la protection des renseignements personnels*, la *Loi sur l'accès à l'information*, le *Règlement sur le recyclage des produits de la criminalité*, la *Loi sur le financement d'activités terroristes* et la *Loi sur les archives nationales du Canada*;
2) Les politiques pertinentes du gouvernement en matière de sécurité;
3) Les politiques pertinentes du gouvernement en matière de protection des renseignements personnels.

Les renseignements personnels connexes à la délivrance de certificats dans le cadre des présentes politiques de certification sont considérés comme étant de nature particulièrement délicate.

Les renseignements relatifs à la révocation/suspension de certificats, en particulier les codes de raison, peuvent être versés dans une LCR. Les certificats et les LCR ne sont pas considérés comme des renseignements personnels aux fins des présentes politiques de certification.

2.5.2 Collecte permise de renseignements personnels

L'AC ne recueillera pas de renseignements personnels pour une autre fin que celle liée à la délivrance et à la gestion de certificats à du personnel de l'AC ou à tout fournisseur de services d'AC, à toute AE ou à toute entité finale. L'AC ne recueillera pas plus de renseignements que ceux dont elle a besoin à cette fin.

2.5.3 Utilisation permise de renseignements personnels

L'AC utilisera seulement les renseignements personnels recueillis par l'AC aux fins de délivrance et de gestion d'un certificat dans le cadre des présentes politiques de certification.

2.5.4 Distribution permise de renseignements personnels

Compte tenu des dispositions énoncées aux sections 2.5.6 et 2.5.7 ainsi que des limitations et des permissions prévues dans la *Loi sur la protection des renseignements personnels* et d'autres lois, politiques et règlements pertinents, l'AC et toute AE peuvent distribuer des renseignements personnels au personnel de CANAFE seulement qui en a besoin pour aider à la délivrance et à la gestion de certificats.

L'AC ou toute AE peut divulguer des renseignements personnels s'il existe, de l'avis de l'AC ou de l'AE, une urgence constituant une menace pour la vie.

2.5.5 Possibilité du propriétaire à corriger des renseignements personnels

Le propriétaire de renseignements personnels ou un organisme client, suivant les besoins, peut corriger toute inexactitude ou demander toute correction au sujet des renseignements personnels fournis par le propriétaire, et ce en tout temps. L'AC et toute AE désigneront une personne qui sera responsable de la réception des demandes afin de corriger tout renseignement personnel connexe à l'ICP et publiera les renseignements sur les contacts dans son site Web ou selon toute manière convenant aux circonstances particulières.

2.5.6 Divulgation de renseignements personnels à des responsables de l'application de la loi

L'AC ou toute AE divulguera tout renseignement personnel, recueilli à la seule fin de délivrer et de gérer un certificat, à des responsables de l'application de la loi, et ce sur réception (1) d'un avis juridique; (2) du consentement du propriétaire des renseignements personnels; ou (3) suivant les besoins ou selon les permissions accordées par une autorité légalement compétente expresse.

2.5.7 Divulgation de renseignements personnels lors de poursuites judiciaires

L'AC ou toute AE divulguera seulement tout renseignement personnel, recueilli afin de délivrer et de gérer un certificat, lorsqu'on le lui demandera en rapport avec des poursuites judiciaires, sur réception (1) d'un avis juridique; (2) du consentement du propriétaire des renseignements personnels; ou (3) suivant les besoins ou selon les permissions accordées par une autorité légalement compétente expresse.

2.6 Responsabilité financière

Dans l'éventualité où l'AC établit un contrat pour obtenir des services d'AC, elle doit s'assurer que les fournisseurs de services présentent la preuve satisfaisante de la responsabilité financière et, le cas échéant, renoncent à toute immunité prévue par la loi.

2.7 Interprétation et mise en vigueur

2.7.1 Loi applicable

Les lois du Canada et les lois applicables des provinces et des territoires, à l'exclusion des principes sur les conflits de lois, régissent la mise en vigueur, la construction, l'interprétation et la validité des présentes politiques de certification.

Toute entente intervenue avec l'AC doit être régie par les lois du Canada et par les lois applicables des provinces et des territoires, à l'exclusion des principes sur les conflits de lois, régissant la mise en vigueur, la construction, l'interprétation et la validité des présentes politiques de certification.

2.7.2 Procédures de règlement de différends

Si un différend surgit entre CANAFE et l'abonné, les parties tenteront de le régler à l'amiable.

2.8 Droits à acquitter

Sans objet.

2.9 Droits de propriété intellectuelle

Tous les droits, titres et intérêts liés à des droits de propriété intellectuelle décrits dans les présentes politiques de certification, les LCR, les LCAR, les noms distinctifs, les dispositions relatives à des services de CANAFE, les clés publiques de l'AC et les certificats ainsi que les certificats des entités finales (le « matériel ») ou connexes à ces éléments, y compris toutes les modifications et les améliorations apportées à celles-ci, sont et doivent demeurer la propriété exclusive de CANAFE.

Les abonnés, les détenteurs de certificats désignés et les parties utilisatrices peuvent utiliser le matériel aux seules fins de se conformer aux présentes politiques de certification. Tout autre emploi commercial ou non est strictement interdit. Les PC peuvent être copiées et distribuées, pourvu que tous les avis concernant les droits d'auteur ou d'autres avis de propriété, le cas échéant, soient préservés ou qu'une reconnaissance équivalente accompagne ces documents quant à leur origine et à leur propriété.

Tout logiciel fourni de pair avec l'emploi du matériel est la propriété de CANAFE ou de ses détenteurs de licences tiers. L'emploi d'un tel logiciel sera conforme aux conditions de la licence applicable au logiciel.

2.10 Réglementation concernant les produits de chiffrement

L'exportation ou l'importation de logiciels servant à valider la fourniture des services offerts par l'AC peuvent nécessiter l'approbation des autorités gouvernementales appropriées. Quiconque utilise les services offerts par l'AC se conformera aux lois et aux règlements applicables concernant l'exportation et l'importation. L'AC ne sera pas responsable d'obtenir toute permission concernant une telle exportation ou une telle importation de logiciels ou d'aviser les utilisateurs au sujet de l'existence ou du contenu d'une telle permission.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1 Désignation

3.1.1 Types de noms

Conformément au certificat X.509 du GC et au profil concernant les champs et les extensions des LCR, chaque entité :

a) Doit détenir un nom distinctif (ND) x.501 facile à distinguer et unique dans le champ de nom de sujet du certificat;

b) Peut utiliser un nom de rechange grâce au champ « SubjectAlternativeName ».

Le ND doit se présenter sous la forme d'une chaîne imprimable X.501 et ne doit pas être vide.

3.1.2 Obligation d'utiliser des noms significatifs

Le nom « Subject » dans un certificat doit être significatif dans la mesure où CANAFE a associé le certificat à une entité finale.

3.1.3 Anonymat des abonnés et des détenteurs de certificats désignés

Le nom distinctif relatif (NDR) peut, malgré que cela ne soit pas nécessaire, désigner de manière visible le nom légal ou organisationnel d'une entité finale. Les noms légaux, les noms organisationnels, les identificateurs alphanumériques ou les chiffrements des éléments précédents peuvent servir de NDR.

Lorsqu'un nom légal ou organisationnel n'est pas utilisé comme NDR d'un certificat, l'AC doit s'assurer qu'un registre est conservé du nom de la personne détenant un certificat ou, dans le cas d'un certificat pour un dispositif, un rôle ou une application, étant responsable de ce certificat.

3.1.4 Règles d'interprétation des diverses formes de noms

Les règles d'interprétation des diverses formes de noms seront conformes au schéma des annuaires communs du GC, version 1.2, daté du 30 novembre 2000, comme il a été modifié ou révisé.

Le fait qu'un nom soit épelé sans ses caractères accentués n'empêche pas sa conformité au nom officiel.

3.1.5 Unicité des noms

Les noms distinctifs doivent être uniques pour toutes les entités finales de l'AC. On n'aura pas recours au champ « SubjectUnique Identifiers », comme il est défini dans le certificat sur l'infrastructure à clé publique X.509 d'Internet et le profil des LCR afin de distinguer des abonnés dont le nom est identique.

L'AC se réserve le droit de prendre des décisions relativement aux noms d'entités pour tous les certificats attribués. Une partie demandant un certificat peut devoir démontrer qu'elle a le droit d'utiliser un nom particulier.

En cas de différend quant au nom dans un dépôt non sous son contrôle, l'AC doit s'assurer dans son entente avec ce dépôt que celui-ci présente une procédure de résolution des différends concernant la revendication des noms.

3.1.6 Reconnaissance, authentification et rôles des marques de commerce

Si cela est permis ou nécessaire, l'emploi d'une marque de commerce est réservé au détenteur de cette marque.

3.2 Validation initiale de l'identité

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

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Avant la délivrance d'un certificat de vérification, l'AC et l'entité finale confirmeront leur identité respective de manière sûre.	Avant l'échange d'une clé privée de chiffrement, l'AC et l'entité finale confirmeront leur identité respective de manière sûre.

3.2.2 Authentification de l'identité d'un organisme

Un organisme doit déposer une demande d'abonnement par l'entremise d'une personne agissant en son nom.

L'identité d'un organisme doit être authentifiée d'une manière qui assurera à l'AC que l'organisme présente l'identité qu'elle prétend détenir. L'authentification de l'identité de l'organisme peut être obtenue à l'aide de l'un ou l'autre des moyens suivants :

a) Renseignements partagés en privé si l'identité de l'organisme a déjà été établie par CANAFE; ou

b) Copies de la documentation officielle fournissant la preuve de l'existence de l'organisme.

L'AC ou l'AE doit également vérifier l'autorité de la personne agissant au nom de l'organisme (c.-à-d. la personne responsable chez le client (PRC)).

L'AC ou l'AE doit s'assurer qu'un dossier est conservé des moyens d'établissement de la PRC.

3.2.3 Authentification de l'identité d'une personne

Personnes agissant en leur nom

Une demande déposée par une personne désirant devenir un abonné et agir en son nom (« abonné éventuel ») doit être présentée par la personne ou par une autre personne autorisée à agir au nom de l'abonné éventuel.

L'identité d'un abonné éventuel doit être authentifiée d'une manière qui assurera à l'AC ou à l'AE que la personne présente l'identité qu'elle prétend détenir. L'AC ou l'AE peut authentifier l'identité d'un abonné éventuel de l'un ou l'autre des moyens suivants :

a) Renseignements partagés en privé si l'identité de la personne a déjà été établie par CANAFE aux fins d'enregistrement;

b) Deux pièces d'identité (copies notariées ou originaux) dont l'une doit être une identification délivrée par le gouvernement fédéral et comportant une photographie; ou

c) Copies certifiées de deux pièces d'identification accompagnées de l'attestation d'une personne autorisée à agir comme garant pour une demande de passeport canadien afin de confirmer, à sa connaissance, que la prétendue personne présente l'identité qu'elle prétend détenir.

L'AC ou l'AE doit s'assurer qu'un dossier est conservé des moyens d'établissement de l'identité de la personne et de tout type d'identification utilisé. Cependant, l'AC ou l'AE n'est pas tenue de conserver une copie de l'identification.

Personne considérée comme détenteur de certificat désigné au sein d'un organisme client

Une demande, visant à demander à ce qu'une personne soit considérée comme un détenteur de certificat désigné agissant au nom d'un organisme client, doit être approuvée par une personne responsable chez le client (PRC) avant d'être présentée à l'AC. La PRC doit se conformer aux exigences de l'AE énoncées dans les présentes politiques de certification.

L'identité d'une personne doit être authentifiée d'une manière qui assurera à la PRC que la personne présente l'identité qu'elle prétend détenir. Une PRC doit fournir les renseignements suivants à l'AC :

a) Renseignements d'identification de la personne;

b) Attestation que l'identification et l'authentification ont été effectuées;

c) Renseignements sur les contacts afin de permettre à l'AC ou à l'AE de communiquer avec l'abonné et la PRC.

3.3 Identification et authentification de demandes de renouvellement d'une clé

3.3.1 Identification et authentification pour le renouvellement routinier d'une clé

Une demande de renouvellement d'une clé peut être présentée par l'entité pour laquelle les clés ont été délivrées ou par une autre personne autorisée à agir en son nom. Toutes ces demandes doivent être authentifiées par l'AC et la réponse subséquente doit être authentifiée par l'entité ou par l'autre personne autorisée à agir en son nom.

Une entité demandant le renouvellement d'une clé peut authentifier la demande à l'aide de sa paire de clés de signature numérique.

En cas d'expiration de l'une des clés, la demande de renouvellement doit être authentifiée de la même façon que s'il s'agissait d'un enregistrement initial.

Les demandes de renouvellement de clés doivent être consignées dans un journal.

3.3.2 Identification et authentification pour le renouvellement d'une clé par suite d'une révocation

Lorsque les renseignements présentés dans un certificat ont changé ou qu'il existe une atteinte à l'intégrité connue ou soupçonnée d'une clé privée, l'AC doit authentifier le renouvellement d'une clé comme s'il s'agissait d'un enregistrement initial.

Tout changement apporté aux renseignements présentés dans un certificat doit être vérifié par l'AC ou une AE autorisée à agir en son nom, et ce avant la délivrance du certificat, exception faite du cas où l'AC a déterminé que de nombreux changements apportés aux ND des abonnés ou aux détenteurs de certificats désignés résultent de changements organisationnels au sein de l'organisme client.

Les demandes de renouvellement de clés par suite d'une révocation doivent être consignées dans un journal.

3.4 Identification et authentification d'une demande de révocation

Une demande de révocation peut être présentée par l'entité pour laquelle les clés ont été délivrées ou par une autre personne autorisée à agir en son nom.

L'AC ou l'AE doit authentifier une demande de révocation d'un certificat. L'authentification peut être effectuée à l'aide de renseignements partagés en privé.

Une entité demandant la révocation peut authentifier la demande à l'aide de sa paire de clés de signature numérique valide.

L'AC doit établir et rendre publics le processus de traitement d'une telle demande et les moyens d'établissement de la demande.

Les demandes de révocation de certificats doivent être consignées dans un journal.

3.5 Identification et authentification d'une demande de récupération

Une demande de récupération peut être présentée par l'entité pour laquelle les clés ont été délivrées ou par une autre personne autorisée à agir en son nom.

L'AC ou l'AE doit authentifier toutes les demandes déposées par des abonnés en vue d'une récupération d'un ESP ou d'une clé privée de confidentialité. L'authentification peut être effectuée à l'aide de renseignements partagés en privé.

La récupération d'un ESP ou d'une clé peut être effectuée à l'aide d'un processus automatisé. L'AC communiquera aux abonnés et aux détenteurs de certificats désignés le processus automatisé ou manuel permettant de déposer des demandes de récupération et d'authentifier de telles demandes.

Une entité demandant la récupération peut authentifier la demande à l'aide de sa paire de clés de signature numérique valide.

Les demandes de récupération d'un ESP ou d'une clé doivent être consignées dans un journal.

4. EXIGENCES OPÉRATIONNELLES CONCERNANT LA DURÉE DE VIE DE CERTIFICATS

4.1 Demande de certificats

L'AC doit :

1) Préciser dans l'ÉPC toutes les procédures et exigences relatives aux demandes de délivrance de certificats;
2) Informer les détenteurs de certificats éventuels au sujet des renseignements qu'ils doivent présenter et du processus à suivre pour les demandes.

L'AC doit s'assurer que des conditions d'emploi régissent chaque certificat qu'elle délivre. Les abonnés doivent passer des ententes ou autrement être soumis aux conditions concernant leurs droits, leurs privilèges et leurs obligations relativement aux certificats qui leur sont délivrés.

Lors du dépôt d'une demande à l'intention d'un détenteur de certificat désigné, une PRC fera référence au nom de l'organisme client, à la date d'exécution de l'entente ou à tout identificateur de contrat, afin de faire mention de l'entente que leur organisme a signé a trait aux droits, aux privilèges et aux obligations associés aux certificats délivrés ou à délivrer à l'intention des détenteurs de certificats désignés agissant au nom de l'organisme client.

Une demande de certificat n'entraîne pas nécessairement sa délivrance par l'AC. CANAFE se réserve le droit de refuser de délivrer un certificat.

4.2 Délivrance de certificats

La délivrance d'un certificat par l'AC indique que la demande de certificat a été entièrement et finalement approuvée par l'AC.

4.3 Acceptation de certificats

L'emploi du certificat par un abonné, par un détenteur de certificat désigné ou par un rôle, par un dispositif ou par une application détenant un certificat constitue l'acceptation de celui-ci et de toutes les obligations connexes.

4.4 Révocation ou suspension de certificats

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
En cas d'atteinte à l'intégrité de la clé de signature de l'AC, l'AC se conformera aux obligations décrites à la section 5.7.3. En cas d'atteinte à l'intégrité réelle ou soupçonnée de toute clé de signature de l'entité, l'entité doit en aviser immédiatement l'AC.	En cas d'atteinte à l'intégrité réelle ou soupçonnée de la clé privée de chiffrement de l'entité, l'entité doit en aviser immédiatement l'AC.

4.4.1 Circonstances conduisant à la révocation

Après la réception d'un avis acceptable, l'AC révoquera un certificat dans les circonstances suivantes :

1) Lorsque tout renseignement du certificat est modifié;
2) Lorsqu'on soupçonne une atteinte à l'intégrité de la clé privée ou du support la renfermant, ou que l'on en est assuré;
3) Lors du décès d'un abonné; ou
4) Lors du décès ou de la cessation d'emploi d'un détenteur de certificat désigné.

L'AC peut, à sa discrétion, révoquer un certificat quand une entité ne se conforme pas à une entente ou à toute loi applicable ou lorsque l'AC croit raisonnablement que cela se prête aux circonstances. L'AC avisera une entité de la révocation d'un certificat qui lui a été attribué.

4.4.2 Qui peut demander une révocation

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

1) Un abonné ou un détenteur de certificat désigné;
2) Une personne autorisée à agir au nom de l'abonné ou à qui le certificat a été délivré;
3) Une personne responsable chez le client d'un certificat délivré à une personne, à un rôle, à un dispositif ou à une application au sein de l'organisme client;
4) Le personnel de l'AC; ou
5) Une AE, à la demande d'un abonné ou d'une personne responsable chez le client.

4.4.3 Procédure de demande de révocation

L'AC doit :

1) Authentifier toutes les demandes de révocation;
2) Consigner et conserver tous les renseignements propres à de telles demandes, y compris un énoncé quant à la mesure prise par l'AC;
3) Publier un avis concernant la révocation d'un certificat dans sa LCR.

4.4.4 Délai de grâce pour une demande de révocation

Toute mesure prise par suite d'une demande de révocation d'un certificat doit être initiée :

1) Immédiatement, si la demande est reçue pendant les heures ouvrables habituelles de l'AC;
2) Immédiatement le jour ouvrable suivant, si la demande est reçue à l'extérieur des heures ouvrables régulières.

4.4.5 Circonstances justifiant la suspension

L'AC peut mette en place l'équivalent d'une suspension par révocation lorsque le code de motif est « en suspens ». La révocation temporaire d'un certificat n'affecte pas les obligations d'un abonné en ce qui concerne la clé privée associé au certificat.

L'AC révoquera temporairement un certificat en cas d'atteinte à l'intégrité soupçonnée de la clé privée ou du support la renfermant.

L'AC peut, à sa discrétion, révoquer temporairement un certificat lorsqu'une entité ne se conforme pas à une entente ou à toute loi applicable ou lorsque l'AC croit raisonnablement que cela se prête aux circonstances.

4.4.6 Qui peut demander une suspension

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

1) Un abonné ou un détenteur de certificat désigné;
2) Une personne autorisée à agir au nom de l'abonné ou à qui le certificat a été délivré;
3) Une personne responsable chez le client ou un détenteur de certificat désigné au sein de l'organisme client, dans le cas d'un certificat délivré à une personne, à un rôle, à un dispositif ou à une application au sein de l'organisme;
4) Le personnel de l'AC; ou
5) Une AE, à la demande d'un abonné, d'un détenteur de certificat désigné ou d'une personne responsable chez le client.

4.4.7 Procédure de demande de suspension

L'AC doit :

1) Authentifier toutes les demandes de révocation temporaire de certificats;
2) Consigner et conserver tous les renseignements propres à de telles demandes, y compris un énoncé quant à la mesure prise par l'AC;
3) Publier un avis concernant la révocation temporaire d'un certificat dans sa LCR.

4.4.8 Limites de la période de suspension

L'AC peut mettre fin à la révocation temporaire d'un certificat lorsqu'elle détermine que les motifs l'y ayant conduit n'étaient pas fondés.

4.4.9 Fréquence de délivrance d'une LCR

L'AC émettra une LCR à jour au moins toutes les vingt-quatre (24) heures. L'AC doit également s'assurer que l'émission de sa LCR est synchronisée à celle de tous les dépôts pertinents, et ce afin de permettre à une partie utilisatrice d'obtenir la LCR la plus récente.

En cas d'atteinte à l'intégrité réelle ou soupçonnée d'une clé, l'AC émettra une LCR à jour immédiatement après la révocation d'un certificat.

4.4.10 Exigences de vérification d'une LCR

Une partie utilisatrice doit :

1) Vérifier l'état de tous les certificats de la chaîne de validation de certificats en le comparant aux LCR actuelles avant de se fier à de tels certificats;
2) Vérifier l'authenticité et l'intégrité des LCR.

5. CONTRÔLES DES INSTALLATIONS, DE LA GESTION ET DES ACTIVITÉS

5.1 Contrôles matériels

5.1.1 Emplacement et construction du site

L'AC doit s'assurer que l'emplacement des installations informatiques hébergeant les services de l'AC, y compris les autorités d'enregistrement automatisées :

1) Satisfont, à tout le moins, aux exigences de zone de sécurité;
2) Sont surveillées à la main ou par des moyens électroniques pour toute intrusion non autorisée, et ce en tout temps.

5.1.2 Accès physique

En ce qui concerne l'emplacement du matériel et des logiciels de l'AC, l'AC doit s'assurer des aspects suivants :

1) Que l'accès non escorté au serveur de l'AC est limité au personnel désigné dans une liste d'accès;
2) Que le personnel ne figurant pas sur la liste d'accès est escorté et supervisé de manière convenable;
3) Qu'un journal d'accès au site est tenu à jour et inspecté de façon régulière.

L'AC doit s'assurer que tous les supports et documents renfermant des renseignements de nature délicate en texte intégral sont stockés dans des conteneurs énumérés dans le *Guide d'équipement de sécurité* du GC ou dans des conteneurs dont la force est équivalente à ceux présentés dans le Guide.

Lorsqu'un NIP ou un mot de passe est consigné au sujet du site de l'AC ou de l'AE, il doit être stocké dans un conteneur de sécurité accessible seulement par le personnel autorisé.

5.1.3 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.

5.1.4 Exposition à l'eau

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

5.1.5 Prévention et protection contre les incendies

L'AC doit s'assurer que le système de l'AC est protégé de manière adéquate contre les incendies par un système d'extinction incendie.

5.1.6 Supports de stockage

L'AC doit s'assurer que les supports de stockage servant au système de l'AC est protégé contre les menaces environnementales comme la température, l'humidité et le magnétisme.

5.1.7 Élimination des données

L'AC doit s'assurer que tous les supports renfermant des renseignements de nature délicate sont nettoyés afin de supprimer l'information de sorte que la récupération des données ne soit pas possible ou que celles-ci soient détruites avant l'élimination. Le personnel de l'AC rendra compte de la destruction des renseignements de nature délicate.

5.1.8 Sauvegarde à l'extérieur du site

L'AC doit s'assurer :

1) Que les installations utilisées pour la sauvegarde à l'extérieur du site et pour l'archivage :
   a) Sont du même niveau de sécurité que le site primaire de l'AC;
   b) Présentent une protection adéquate contre les menaces environnementales comme la température, l'humidité et le magnétisme.
2) Que la transmission et/ou le transport de matériel en vue de la sauvegarde ou de l'archivage par l'AC vers le site de sauvegarde à l'extérieur du site sont menés de manière sûre.

5.2 Contrôles procéduraux

5.2.1 Rôles confiés

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 (3) rôles distincts du personnel pour l'ICP, pour distinguer les activités quotidiennes du système de l'AC, la gestion de ces activités ainsi que la gestion des modifications d'importance des exigences, y compris les politiques, les procédures ou le personnel. Ces rôles doivent être joués par le personnel désigné comme étant le suivant :

a) Utilisateur maître de l'ICP;

b) Agent de l'ICP;

c) Administrateur de l'ICP,

et présentant, au moins, les responsabilités définies à la section 1.3.1. Toute autre répartition des responsabilités est permise dans la mesure où elle offre le même niveau de résistance à une « attaque intérieure ».

Seul l'utilisateur maître de l'ICP et le personnel responsable de la configuration du matériel et des logiciels de systèmes d'exploitation, ou encore le personnel escorté par eux, doivent détenir un accès physique au logiciel de contrôle du système de l'AC.

Le personnel de l'AC ne vérifiera pas ses propres activités.

5.2.2 Nombre de personnes nécessaires par tâche

L'AC doit s'assurer que personne ait accès aux clés privées de l'abonné stockées par l'AC. Au moins deux personnes accompliront les tâches de nature délicate, celles-ci étant définies dans l'ÉPC. L'AC peut permettre aux abonnés et aux détenteurs de certificats désignés de procéder eux-mêmes de manière sûre à la récupération de leurs clés ou à la révocation des certificats.

Le contrôle de clés par plusieurs utilisateurs est également nécessaire pour la production des clés de l'AC, comme il est défini à la section 6.2.2. Compte tenu de la section 5.2.1, une personne peut accomplir toutes les autres tâches associées aux rôles de l'AC.

5.2.3 Identification et authentification de chaque rôle

L'identité et l'autorisation du personnel de l'AC seront vérifiées avant :

1) de figurer dans la liste d'accès au site de l'AC;
2) de figurer dans la liste d'accès pour l'accès physique au système de l'AC;
3) d'obtenir un certificat pour l'accomplissement de son rôle à l'AC;
4) de lui allouer un compte sur le système de l'ICP, si un tel compte est nécessaire.

Chacun de ces certificats ou comptes, exception faite du certificat de signature de l'AC :

1) Pourra être attribué directement à une personne;
2) Ne doit pas être partagé avec une autre personne;
3) Ne servira à aucune autre fin que celle liée à l'accomplissement des tâches attribuées au personnel de l'AC détenant de tels certificats ou comptes.

L'AC mettra en place ces exigences à l'aide des contrôles procéduraux et des logiciels du système d'exploitation et de l'AC.

5.3 Contrôles du personnel

L'AC doit s'assurer que le personnel accomplissant les tâches liées à l'exploitation de l'AC ou une AE sont embauchés à contrat ou reconnaissent autrement les conditions de leur embauche. L'AC doit s'assurer que de telles conditions d'embauche comportent une exigence de la part de tel personnel de ne pas divulguer les renseignements de nature délicate particuliers à la sécurité de l'AC ou des renseignements personnels selon la définition qui est donné de ce terme à la section 2.5.1.

L'AC doit s'assurer qu'elle ne confie pas de tâches à du personnel qui risqueraient d'entrer en conflit avec celles qu'il accomplit auprès de l'AC ou de l'AE.

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

L'AC doit s'assurer que tout le personnel remplissant des fonctions de nature délicate pour une AC ou une AE détient les connaissances, l'expérience et les compétences nécessaires pour accomplir celles-ci.

L'AC doit s'assurer que tout le personnel lié à l'exploitation de la l'AC détient une habilitation de sécurité et est autorisé à accéder à des renseignements de nature secrète.

5.3.2 Procédures de vérification des connaissances

Toutes les vérifications des connaissances doivent être effectuées 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 reçoive la formation pertinente. Une telle formation devrait porter sur des sujets d'intérêt comme les exigences en matière de sécurité, les responsabilités opérationnelles et les procédures connexes.

5.3.4 Fréquence et exigences en matière de renouvellement de la formation

L'AC reverra son programme de formation et le mettra à jour, au moins une fois l'an, afin de tenir compte des changements apportés au système de l'AC.

5.3.5 Fréquence et séquence pour la 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'AE, l'AC suspendra l'accès à son système de cette personne.

5.3.7 Exigences concernant les entrepreneurs autonomes

L'AC doit s'assurer que le personnel à contrat satisfait aux mêmes exigences en matière de sécurité du personnel en ce qui concerne la nomination, la formation et les vérifications des connaissances que celles des employés de l'AC.

5.3.8 Documentation fournie au personnel

L'AC mettra à la disposition du personnel de l'AC, des AE et des personnes responsables chez le client les présentes politiques de certification, les dispositions pertinentes de l'ÉPC ainsi que toute autre loi ou politique ou tout autre contrat propres au poste du personnel de l'AC.

5.4 Procédures de consignation des vérifications

5.4.1 Types d'événements consignés

L'AC doit s'assurer qu'elle dispose de la capacité de consigner ou de faire consigner dans des fichiers de journaux de vérification tous les événements liés à la sécurité du système de l'AC, y compris notamment les routeurs, les cloisons pare-feu, les répertoires et les serveurs hébergeant les logiciels de l'AC et de l'AE. Toutes les fonctions de vérification de la sécurité du système d'exploitation de l'AC et des applications de l'AC seront activées.

Ces événements comprennent notamment :

1) Démarrage et arrêt du système;
2) Démarrage et arrêt de l'application de l'AC;
3) Tentatives de créer, de supprimer ou de définir des mots de passe ou de modifier les privilèges du système pour l'utilisateur maître de l'ICP, pour les agents de l'ICP et pour les administrateurs de l'ICP;
4) Modifications apportées aux détails et/ou aux clés de l'AC;
5) Modifications apportées aux politiques de création de certificats (p. ex. période de validité);
6) Tentatives d'ouverture et de fin de séances;

7) Tentatives non autorisées d'accès au réseau depuis le système de l'AC;
8) Tentatives non autorisées d'accès à des fichiers du système;
9) Production des clés de l'AC et d'entités subordonnées;
10) Création et révocation des certificats;
11) Tentatives d'initialiser, de supprimer, de valider et d'invalider les abonnés, ainsi que tentatives de mettre à jour et de récupérer leurs clés;
12) Opérations d'écriture et d'écriture non concluantes relativement à un certificat et à un répertoire des LCR.

Tous les journaux, qu'ils soient électroniques ou manuels, doivent renfermer la date de l'événement et l'identité de l'entité à l'origine de celui-ci.

L'AC recueillera également, par voie électronique ou manuellement, les renseignements de sécurité non produits par le système de l'AC comme les suivants :

1) Journaux de l'accès physique;
2) Modifications apportées à la configuration du système et maintenance, selon la définition donnée dans l'ÉPC;
3) Modifications apportées au personnel de l'AC;
4) Rapports sur les écarts et les situations d'atteinte à l'intégrité;
5) Renseignements concernant la destruction des renseignements de nature délicate;
6) Versions actuelles et antérieures de toutes les politiques de certification;
7) Versions actuelles et antérieures des *Énoncés de pratiques de certification*;
8) Rapports d'inspection sur la conformité.

L'AC indiquera dans l'ÉPC les renseignements à consigner.

Afin de faciliter la prise de décisions, toutes les ententes et toute la correspondance relatives aux services de l'AC seront recueillies et consolidées, par voie électronique ou manuellement, dans un seul emplacement.

5.4.2 Fréquence de traitement des journaux de vérification

L'AC doit s'assurer que tous les événements importants sont expliqués dans un journal de vérification sommaire et que tout le personnel de l'AC examine les journaux de vérification au moins une fois par semaine. De tels examens supposent la vérification que le journal n'a pas encore été violé et passent en revue brièvement toutes les entrées du journal. Le personnel de l'AC mènera une enquête plus approfondie de toute « alerte » ou irrégularité présentes dans les journaux. L'AC indiquera qui est responsable de l'examen des journaux de vérification et de la préparation des journaux de vérification sommaires dans l'ÉPC.

L'AC devrait examiner le manuel à l'appui et les journaux électroniques, y compris ceux des AE, lorsqu'un geste semble douteux.

L'AC documentera toute mesure prise par suite de ces examens.

5.4.3 Période de conservation du journal de vérification

L'AC conservera ses journaux de vérification sur le site pendant au moins deux (2) mois et, par la suite, ceux produits par le logiciel de l'ICP de la manière décrite à la section 5.5.

5.4.4 Protection du journal de vérification

L'AC protégera le système des journaux de vérification électroniques et les renseignements concernant la vérification manuelle contre toute consultation, modification, suppression ou destructions non autorisées.

5.4.5 Procédures de sauvegarde du journal de vérification

L'AC fera une copie de sauvegarde de tous les journaux et sommaires de vérification, ou en fera une copie si ceux-ci sont présentés dans un format papier.

5.4.6 Système de collecte pour la vérification

L'AC identifiera son système de collecte pour la vérification dans l'ÉPC.

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

Lorsqu'un événement est consigné par le système de collecte pour la vérification, l'AC se réserve le droit de ne pas donner avis à la personne, à l'organisme, au rôle, au dispositif ou à l'application ayant causé l'événement.

5.4.8 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 et prendra les mesures nécessaires afin de réduire au minimum les vulnérabilités désignées du système dès que cela est raisonnablement possible de le faire.

5.5 Archivage des dossiers

Les certificats, les cocertificats et les certificats (autosignés) de l'AC stockés par l'AC ainsi que les LCAR et les LCR produites par l'AC doivent être conservés pendant au moins deux (2) ans après leur expiration.

Les renseignements concernant la vérification dont les détails figurent à la section 5.4 devraient être conservés pendant une période définie dans l'Énoncé de pratiques de certification.

Les renseignements suivants doivent être conservés pendant au moins six (6) ans :

1) Les journaux de vérification produits par le logiciel de l'AC de l'ICP;
2) Les ententes avec les abonnés;
3) Les dossiers concernant les renseignements d'identification et d'authentification;
4) Les journaux concernant l'accès physique;
5) Les modifications apportées à la configuration du système et la maintenance de celui-ci, selon les définitions données dans l'ÉPC;
6) Les modifications apportées au personnel de l'AC;
7) Les rapports sur les écarts et sur l'atteinte à l'intégrité;
8) L'information concernant la destruction de renseignements de nature délicate;
9) Les versions actuelles et précédentes de toutes les politiques de certification;
10) Les versions actuelles et précédentes de l'*Énoncé de pratiques de certification*;
11) Les rapports d'inspection de la conformité.

Les clés privées de confidentialité sauvegardées par l'AC seront protégées à un niveau physique et cryptographique équivalant à celui en place au site de l'AC ou dépassant celui-ci.

Les clés privées de confidentialité qui sont sauvegardées par l'AC seront archivées pendant une période de 10 ans.

L'AC archivera toutes les clés et tous les mots de passe nécessaires pendant une période suffisante pour prendre en charge les responsabilités de l'AC.

Une deuxième copie de tout le matériel conservé ou sauvegardé doit être stockée dans un emplacement autre que le site de l'AC et doit être protégée par un moyen de sécurité matérielle utilisé seul ou en combinaison avec un dispositif de chiffrement.

L'AC vérifiera l'intégrité de toutes les sauvegardes et de tout le matériel stocké à l'extérieur du site, respectivement une fois tous les six (6) mois et une fois l'an.

Outre les points susmentionnés, les renseignements conservés ou sauvegardés par l'AC peuvent être soumis à des exigences concernant leur archivage, conformément à la *Loi sur les archives nationales du Canada*, à d'autres lois applicables et à la politique du GC.

5.6 Renouvellement de clés

L'AC indiquera dans l'ÉPC :

1) La période au cours de laquelle les clés de l'abonné et du détenteur de certificat désigné peuvent être renouvelées avant la date d'expiration du certificat, pourvu que le certificat n'ait pas été révoqué;
2) Le processus par lequel l'AC, l'AE, l'abonné ou le détenteur de certificat désigné peut procéder au renouvellement des clés.

Le changement de clés automatisé est permis.

Les abonnés et les détenteurs de certificats désignés ne détenant pas de clés valides doivent être réauthentifiés de la même manière que lors de l'inscription initiale.

Les clés de l'AC sont renouvelées automatiquement selon la fréquence définie à la section 6.3.2 des présentes politiques de certification.

5.7 Atteinte à l'intégrité et reprise après sinistre

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

L'AC énoncera dans l'ÉPC ou dans tout autre document pertinent les procédures 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 ou disposition avec le dépôt prévoit que le dépôt établisse et documente des procédures afin de traiter de la corruption ou de la perte de ressources informatiques, de logiciels et/ou de données.

5.7.2 Révocation du certificat public d'une entité

S'il faut révoquer le certificat de signature numérique de l'AC, l'AC doit immédiatement en aviser :

1) L'AGP de CANAFE;
2) Toutes ses AE;
3) Tous les abonnés.

Après avoir corrigé les facteurs ayant conduit à la révocation, l'AC pourra produire une nouvelle paire de clés de signature de l'AC et délivrer de nouveau des certificats à toutes les entités, en s'assurant que toutes les LCR sont signées à l'aide de la nouvelle clé.

5.7.3 Atteinte à l'intégrité de la clé de l'AC

En cas d'atteinte à l'intégrité de la clé privée de signature numérique de l'AC et avant la nouvelle production de celle-ci, l'AC doit :

1) En aviser l'AGP de CANAFE;
2) Révoquer tous les certificats délivrés à l'aide de cette clé;
3) Fournir un avis convenable à toutes les parties pertinentes.

Après avoir corrigé les facteurs ayant conduit à l'atteinte à l'intégrité, l'AC pourra produire une nouvelle paire de clés de signature de l'AC et délivrer de nouveau des certificats à toutes les entités, en s'assurant que toutes les LCR et toutes les LCAR sont signées à l'aide de la nouvelle clé.

L'AC indiquera dans l'ÉPC ou dans un document rendu public et dans les ententes convenables la façon dont elle fournira un avis concernant l'atteinte à l'intégrité de sa clé de signature.

5.7.4 Possibilités de poursuivre les activités après un désastre

L'AC préparera et tiendra à jour un plan de poursuite des activités donnant les grandes lignes des étapes à suivre pour rétablir une installation sûre en cas de désastre naturel ou autre.

Le plan de poursuite des activités devrait porter sur les aspects suivants :

1) La définition des rôles et des responsabilités des personnes responsables de l'exécution des diverses composantes du plan;
2) Les conditions d'activation du plan, décrivant le processus à suivre avant l'activation du plan;
3) Les procédures d'urgence décrivant les mesures à prendre par suite d'un incident ayant mis en péril les activités et/ou la vie humaine.
4) Les procédures de traitement de secours décrivant les mesures à prendre afin de déplacer les activités fonctionnelles ou les services de soutien essentiels vers des emplacements distincts et de rétablir le fonctionnement selon les échéances fixées;
5) Les procédures de reprise décrivant les mesures à prendre pour reprendre les activités habituelles;
6) Un calendrier d'entretien précisant comment et quand le plan sera mis à l'essai ainsi que le processus de tenue à jour de celui-ci;
7) Les activités de sensibilisation et de formation conçues pour permettre de comprendre les processus de poursuite des activités et pour s'assurer que les processus continuent d'être efficaces.

Si un dépôt n'est pas sous le contrôle de l'AC, l'AC doit s'assurer que toute entente ou disposition avec le dépôt prévoit que le dépôt établisse et documente un plan de poursuite des activités.

5.8 Cessation de l'AC/changement des activités

Si l'AC cesse ses activités ou qu'elle apporte des changements d'importance à celles-ci, elle communiquera à l'AGP de CANAFE l'identité de toutes les entités à qui elle a délivré des certificats. Un tel avis sera transmis avant ou immédiatement après la cessation ou le changement d'importance des activités.

Si l'AC cesse ses activités, elle prendra des mesures pour conserver ses dossiers, y compris les éléments suivants en deux exemplaires :

1) Les certificats;

2) Les clés privées de confidentialité (le cas échéant);

3) Les certificats autosignés de l'AC;

4) Les renseignements de vérification dont les détails sont présentés à la section 5.4;

conformément aux exigences concernant l'archivage précisées dans les présentes politiques de certification.

6. CONTRÔLES DE SÉCURITÉ TECHNIQUES

L'AC sécurisera toutes les opérations de l'AC à l'aide de mécanismes comme l'authentification et le chiffrement forts lors d'un accès avec un réseau partagé.

6.1 Production et installation de paires de clés

6.1.1 Production de paires de clés

Production de clés de l'AC

L'AC doit s'assurer que la production de clés de l'AC sera :

a) Effectuée par le personnel de rôles de confiance soumis à un contrôle double au moins;

b) Effectuée à l'aide d'un dispositif satisfaisant aux exigences énoncées à la section 6.2.1 ou plus élevées;

c) Effectuée grâce à un algorithme approuvé par l'AGP de CANAFE.

Production de clés de l'AE

L'AC doit s'assurer que la production de clés de l'AE sera :

a) Effectuée à l'aide d'un dispositif satisfaisant aux exigences énoncées à la section 6.2.1 ou plus élevées;

b) Effectuée grâce à un algorithme approuvé par l'AGP de CANAFE.

Production de clés d'un abonné/détenteur de certificat désigné

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Chaque paire de clés de signature numérique doit être produite à l'aide d'un algorithme approuvé par l'AGP de CANAFE.	Chaque paire de clés de confidentialité doit être produite à l'aide d'un algorithme approuvé par l'AGP de CANAFE.

Lorsqu'une paire de clés est produite au nom d'un détenteur de certificat éventuel, l'entité ou le processus ayant permis de produire les clés doit détruire son exemplaire de la paire de clés, et ce d'une manière sûre et après avoir déposé les clés sous la garde d'un détenteur de certificat éventuel.

Les paires de clés pour les entités finales autres que l'AC peuvent être produites à l'aide d'un module de chiffrement logiciel ou matériel.

6.1.2 Délivrance de clés privées à l'abonné/au détenteur de certificat désigné

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Si le détenteur de certificat éventuel ne produit pas la clé privée de signature, l'AC la disposera dans un stockage, et ce manière à ce que seul le détenteur de certificat éventuel y ait accès.	Si le détenteur de certificat éventuel ne produit pas la clé privée de déchiffrement, l'AC la disposera dans un stockage.

6.1.3 Délivrance de clés publiques à un délivreur de certificats

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Si l'AC ne produit pas la clé publique de vérification, l'AC prendra des mesures pour qu'elle lui soit délivrée dans une transaction en ligne, et ce d'une manière sûre documentée dans l'ÉPC.	Si l'AC ne produit pas le clé publique de chiffrement, l'AC prendra des mesures pour qu'elle lui soit délivrée dans une transaction en ligne, et ce d'une manière sûre documentée dans l'ÉPC.

6.1.4 Délivrance de clés publiques de l'AC aux abonnés

La clé publique de vérification de l'AC sera délivrée aux abonnés et aux détenteurs de certificats désignés dans une transaction en ligne, et ce d'une manière sûre documentée dans l'ÉPC.

6.1.5 Taille des clés

L'AC utilisera un RSA d'au moins 1 024 bits (un RSA de 2 048 bits est recommandé) pour sa propre paire de clés de signature. Si possible, les entités finales utiliseront l'algorithme RSA 2048 bits pour leurs paires de clés. Par contre, si cela n'est pas possible, les entités finales utiliseront l'algorithme RSA 1024 bits.

6.1.6 Production de paramètres des clés publiques et vérification de la qualité

Aucune disposition.

6.1.7 Usages visés des clés (conformément au champ x509v3)

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Les clés peuvent être utilisées pour l'authentification et l'intégrité des données et à l'appui de la non-répudiation. Les clés de signature de l'AC sont les seules clés permises pour la signature de certificats et de LCR. Le champ « KeyUsage » des certificats doit être utilisé conformément au champ X.509 et au profil d'extension des certificats et des LCR du GC.	Les clés peuvent être utilisées pour l'échange et l'établissement des clés servant à la confidentialité des séances et des données. Le champ « KeyUsage » des certificats doit être utilisé conformément au champ X.509 et au profil d'extension des certificats et des LCR du GC.

6.2 Protection des clés privées et contrôles pour la conception du module de chiffrement

6.2.1 Normes et contrôles pour le module de chiffrement

Tout module de chiffrement utilisé par l'AC, son personnel, les AE, les abonnés et les détenteurs de certificats désignés doit satisfaire aux exigences suivantes :

1) 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 3 de la FIPS 140-1 ou jugé comme offrant un niveau de fonctionnalité et d'assurance équivalent.

2) 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 FIPS 140-1 ou jugé comme offrant un niveau de fonctionnalité et d'assurance équivalent.

3) Les activités de production et de signature des clés de signature numérique des AE doivent être exercées dans un module de chiffrement matériel coté au moins au niveau 1 de la FIPS 140-1 ou jugé comme offrant un niveau de fonctionnalité et d'assurance équivalent. Les processus d'enregistrement automatisés peuvent être menés dans un module de chiffrement logiciel coté au moins au niveau 1 de la FIPS 140-1 ou jugé comme offrant un niveau de fonctionnalité et d'assurance équivalent, si l'AC est d'avis que la sécurité matérielle du logiciel est adéquate. Toutes les autres activités de chiffrement des AE doivent être exercées dans des modules de chiffrement cotés au niveau 1 de la FIPS 140-1 ou jugés comme offrant un niveau de fonctionnalité et d'assurance équivalent.

4) Les entités finales doivent utiliser les modules de chiffrement validés au moins au niveau 1 de la FIPS 140-1 ou jugés comme offrant un niveau de fonctionnalité et d'assurance équivalent.

5) Tous les modules de chiffrement doivent se verrouiller automatiquement après une période donnée d'inactivité.

6.2.2 Contrôle de clés privées par plusieurs personnes

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Il doit y avoir un contrôle par plusieurs personnes pour les activités de production de clés de l'AC. Deux personnes doivent participer à ce contrôle ou être présentes, dont l'une accomplira les tâches associées au rôle d'utilisateur maître de l'ICP.	Il doit y avoir un contrôle par plusieurs personnes pour la récupération de clés privées. Deux personnes doivent participer à ce contrôle ou être présentes, dont l'une accomplira les tâches associées au rôle d'agent de l'ICP ou d'administrateur de l'ICP.

6.2.3 Entiercement de clés privées

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
L'AC n'entiercera pas les clés privées de signature numérique.	Aucune disposition.

6.2.4 Sauvegarde de clés privées

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Une entité peut sauvegarder sa propre clé privée de signature numérique. Dans un tel cas, la clé doit être copiée sous forme chiffrée et protégée à un niveau non inférieur à celui stipulé pour sa version principale. L'AC ne sauvegardera pas les clés privées de signature des abonnés ou des détenteurs de certificats désignés.	Une entité peut également faire une copie de sa clé privée de déchiffrement. Si les clés de confidentialité sont sauvegardées par l'AC, elle les stockera en lieu sûr sous forme chiffrée.

L'AC indiquera dans l'ÉPC ses procédures de sauvegarde de clés.

6.2.5 Archivage de clés privées

Consultez la section 5.5.

6.2.6 Transfert de clés privées à destination et en provenance d'un module de chiffrement

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Si une clé privée de signature n'est pas produite dans le module de chiffrement de l'entité, elle doit être entrée dans le module de manière sécurisée.	Si une clé privée de déchiffrement n'est pas produite dans le module de chiffrement de l'entité, elle doit être entrée dans le module de manière sécurisée.

6.2.7 Stockage de clés privées dans un module de chiffrement

Les clés privées seront stockées dans un ESP.

6.2.8 Méthode d'activation de clés privées

L'entité doit être authentifiée à l'ESP avant l'activation de la clé privée. L'AC doit s'assurer que les règles d'une politique sur les mots de passe sont en place afin d'exiger l'emploi de mots de passe forts pour l'accès à un ESP. L'AGP de CANAFE peut approuver d'autres méthodes d'authentification pour l'activation de clés privées.

6.2.9 Méthode de désactivation de clés privées

Le module de chiffrement doit désactiver automatiquement la clé privée après une période donnée d'inactivité.

Quand les clés privées sont désactivées, elles doivent être supprimées de la mémoire avant désattribution de celle-ci. Elles doivent également être conservées sous leur forme chiffrée seulement. Tout espace disque ayant servi au stockage des clés doit être écrasé avant de le mettre à la disposition du système d'exploitation.

6.2.10 Méthode de destruction de clés privées

À la fin de l'emploi d'une clé privée, son détenteur doit détruire de manière sûre toutes les copies de celle-ci, dans la mémoire informatique et dans l'espace disque partagé. Puisque les clés sont conservées dans un ESP chiffré, la suppression de l'ESP ou la destruction physique d'un des jetons (le cas échéant) constituent des méthodes sûres de destruction de la clé privée.

6.3 Autres aspects de la gestion de paires de clés

6.3.1 Archivage des clés publiques

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
L'AC conservera tous les certificats des clés publiques de vérification de signatures numériques qu'elle produit.	L'AC conservera tous les certificats des clés publiques de chiffrement qu'elle produit.

6.3.2 Périodes de validité des certificats et d'emploi des paires de clés

Clé/certificat	Longueur de la clé en bits	Période de validité maximale
Certificat et clé publique de vérification de l'autorité de certification	1024/2048	8/20 ans
Clé privée de signature de l'autorité de certification	1024/2048	3/8 ans
Certificat et clé publique de vérification de l'entité finale	2048	12 ans
Clé privée de signature de l'entité finale	2048	3,2 ans
Certificat et clé publique de chiffrement de l'entité finale	2048	12 ans
Clé privée de déchiffrement de l'entité finale	2048	Aucune expiration
Certificat et clé publique de vérification de l'entité finale	1024	6 ans
Clé privée de signature de l'entité finale	1024	3,2 ans
Certificat et clé publique de chiffrement de l'entité finale	1024	6 ans
Clé privée de déchiffrement de l'entité finale	1024	Aucune expiration

6.3.3 Stockage, sauvegarde et récupération de clés de l'AC

L'AC doit s'assurer que ses clés privées demeurent confidentielles et conservent leur intégrité. Plus particulièrement :

1) La clé privée de signature de l'AC sera conservée et utilisée dans un dispositif de chiffrement sûr satisfaisant aux exigences énoncées à la section 6.2.1;

2) La clé privée de signature de l'AC peut être exportée selon une méthode approuvée par le CST, entre un dispositif de chiffrement et un autre satisfaisant aux exigences énoncées à la section 6.2.1;

3) Lorsque la clé privée de signature de l'AC se trouve à l'extérieur du dispositif de création de signatures, celle-ci sera chiffrée;

4) La clé privée de signature de l'AC sera sauvegardée, stockée et récupérée selon le même contrôle par plusieurs personnes que celui utilisé pour la clé d'origine, de telle sorte que la sauvegarde sera stockée de manière sûre dans un emplacement de sauvegarde de l'AC;

5) Lorsque les clés de l'AC sont stockées dans un module matériel de traitement de clés spécialisées, des contrôles d'accès sont en place afin de s'assurer qu'elles ne sont pas accessibles à l'extérieur de ce module.

6.3.4 Récupération de clés par un abonné ou par un détenteur de certificat désigné

L'AC peut permettre à un abonné ou à un détenteur de certificat désigné de récupérer ses clés.

6.4 Données d'activation

6.4.1 Production et installation des données d'activation

Toutes les données d'activation doivent être uniques et imprévisibles.

Les clés et les données d'initialisation peuvent être produites en vrac et seront conservées par l'AC de manière sûre avant la distribution. Après avoir reçu une paire de clés de signature numérique et les données d'initialisation associées, un abonné ou un détenteur de certificat désigné doit utiliser les données d'initialisation de manière opportune.

6.4.2 Protection des données d'activation

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

L'Environnement de sécurité personnelle des entités doit être protégé de l'emploi non autorisé à l'aide de mécanismes de chiffrement.

Les données d'activation, de pair avec tout contrôle d'accès, doivent être d'un niveau de protection convenable pour la protection des clés ou des données. Lorsque des mots de passe sont utilisés, l'AC doit s'assurer que le système et/ou les applications d'ICP mettent en vigueur une politique sur les mots de passe forts. Le niveau de protection doit être adéquat afin de décourager un pirate motivé possédant des ressources importantes.

En présence d'un modèle de mots de passe réutilisables, le mécanisme comportera une installation permettant de verrouiller temporairement le compte après un certain nombre donné de tentatives infructueuses.

Une entité doit pouvoir changer son mot de passe en tout temps.

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

Le serveur de l'AC doit comprendre la fonctionnalité suivante en matière de sécurité :

1) Contrôle d'accès aux services de l'AC et aux rôles de l'ICP;
2) Séparation obligatoire des tâches pour les rôles de l'ICP;
3) Identification et authentification des rôles de l'ICP et des identités connexes;
4) Réutilisation ou séparation d'objets pour la mémoire à accès aléatoire de l'AC;
5) Emploi du chiffrement pour la communication entre séances et la sécurité des bases de données, suivant les besoins;
6) Archivage des données historiques et de vérification de l'entité finale et de l'AC;

7) Vérification des événements liés à la sécurité;

8) Validation automatique et régulière de l'intégrité des bases de données de l'AC;

9) Mécanismes de chemins de confiance pour l'identification et l'authentification des rôles de l'ICP et des identités connexes;

10) Mécanismes de récupération pour les clés et le système de l'AC;

11) Renforcement du système d'exploitation 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

Le Centre de la sécurité des télécommunications (CST) ou tout autre laboratoire accrédité d'une tierce partie doit évaluer les éléments critiques en matière de sécurité de l'AC.

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 structurée.

Les processus de conception et d'élaboration doivent être appuyés de la vérification par une tierce partie en ce qui a trait à leur conformité et être accompagnés d'évaluations de la menace et des risques, afin d'influer sur la conception de mesures de sécurité et de réduire au minimum le risque résiduel.

Le matériel ou les logiciels achetés seront expédiés ou livrés dans un contenant scellé dans un emballage moulant et seront installés par du personnel formé.

6.6.2 Contrôles de gestion de la sécurité

Le matériel et les logiciels de l'AC seront spécialisés afin d'accomplir seulement les tâches associées à l'AC. Aucune autre application ni aucun autre dispositif matériel, ni aucune connexion réseau ou composante ne doivent faire partie du fonctionnement de l'AC.

L'AC indiquera dans l'ÉPC ses politiques et ses procédures afin d'empêcher le chargement de logiciels malveillants dans l'équipement de l'AC. L'AC et l'AE ainsi que les logiciels d'enregistrement automatisé seront balayés pour déceler tout code malveillant, et ce lors du premier emploi et périodiquement par la suite.

L'AC utilisera la méthodologie officielle de gestion de la configuration pour l'installation et la maintenance continue du système de l'AC. Les logiciels de l'AC, lorsqu'ils sont chargés pour la première fois, doivent fournir une méthode permettant à l'AC de vérifier que les logiciels du système :

1) Émanent du développeur de logiciels;

2) N'ont pas été modifiés avant l'installation;

3) Constituent la version voulue aux fins d'emploi.

L'AC fournira un mécanisme de vérification périodique de l'intégrité de sa base de données. L'AC disposera également de mécanismes et de politiques pour contrôler et pour surveiller la configuration de son système.

Lors de l'installation et au moins une fois par semaine, l'intégrité de la base de données de l'AC doit être validée.

6.7 Contrôles de sécurité de réseau

L'AC doit s'assurer que des contrôles de sécurité sont en place pour assurer l'intégrité et la disponibilité de l'AC grâce à un réseau ouvert ou polyvalent général auquel elle est connectée. Une telle protection doit comprendre l'installation d'un ou de plusieurs dispositifs configurés de manière à permettre seulement l'emploi des protocoles et, au choix de l'AC, des commandes nécessaires à ses activités. Tout logiciel réseau présent doit être nécessaire au déroulement des activités de l'AC.

L'AC précisera dans l'ÉPC de tels protocoles et, suivant les besoins, les commandes nécessaires au fonctionnement de l'AC.

6.8 Horodatage

L'AC peut permettre ou autoriser quiconque à permettre aux abonnés d'horodater leurs opérations.

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 ou de version ultérieure si l'AGP de CANAFE le lui autorise.

Les logiciels des entités finales de l'ICP doivent prendre en charge tous les champs X.509 (sans extension) de base :

Nom du champ	**Description**
Signature	Signature de l'AC pour authentifier le certificat
Issuer	Nom de l'AC
Validity	Date d'activation et d'expiration du certificat
Subject	Nom distinctif de l'abonné
Subject Public Key Information	Clé d'identification de l'algorithme
Version	Version du certificat X.509
Serial Number	Numéro de série unique pour le certificat

7.1.2 Extensions des certificats

Les règles d'inclusion, d'affectation de valeurs et de traitement d'extensions sont définies dans les profils. Les extensions de certificats utilisées dans les certificats délivrés dans le cadre des présentes politiques de certification seront conformes aux parties applicables des champs et du profil d'extension des LCR et des certificats X.509 de l'ICP du GC.

Les AC afficheront les champs et le profil d'extension des LCR et des certificats X.509 de l'ICP du GC dans leur site Web et indiqueront leur emplacement aux abonnés et aux détenteurs de certificats désignés. Si des extensions privées sont utilisées, elles seront précisées dans l'ÉPC. Les extensions privées critiques seront interopérantes au sein du groupe d'utilisation visé.

7.1.3 Identificateurs d'objets d'algorithmes

L'AC et les entités finales utiliseront seulement les algorithmes approuvés par l'AGP de CANAFE. L'AC utilisera les algorithmes symétriques suivants que prendront en charge par ailleurs les entités finales :

Chiffrement	
Algorithme	**Observations**
Triple DES	L'option à 3 clés indépendantes offre la meilleure sécurité et constitue donc l'option de choix. L'option à 2 clés est également acceptable lorsque la clé utilisé pour le chiffrement final est la même que celle du premier chiffrement. L'option à clé unique n'est pas acceptable, car la sécurité est ainsi limitée à celle d'un algorithme DES à passe unique.

	La période chiffrement d'une clé ne devrait pas dépasser sept jours.
CAST 5/80 ou CAST 5/128	Les modes d'exploitation acceptables sont les mêmes que ceux précisés à l'origine pour l'algorithme DES. La période de chiffrement d'une clé ne devrait pas dépasser vingt-quatre heures.

La liste des algorithmes symétriques à utiliser par toutes les entités de l'ICP peut changer sans entraîner la délivrance d'une nouvelle politique de certification ou la modification de l'IDO de la PC.

Dans l'éventualité d'un changement apporté aux algorithmes approuvés, l'AC doit s'assurer que les abonnés et les détenteurs de certificats désignés sont tenus au courant des changements de la liste des algorithmes approuvés pour CANAFE. L'AC indiquera dans son ÉPC la façon dont elle communiquera de tels avis de changements.

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

Lorsqu'une extension liée à des contraintes de noms est utilisée, celle-ci doit être précisée et traitée de la manière décrite dans les champs et le profil d'extension des LCR et des certificats X.509 de l'ICP du GC.

7.1.6 Identificateur d'objet des politiques de certification

L'AC doit s'assurer que l'IDO des politiques est incluse dans les certificats qu'elle délivre.

7.1.7 Emploi d'une extension de contraintes de politiques

Lorsqu'une extension « policyConstraint » est utilisée, celle-ci doit être précisée et traitée de la manière décrite dans les champs et le profil d'extension des LCR et des certificats X.509 de l'ICP du GC.

7.1.8 Syntaxe et sémantique des qualificateurs de politiques

Lorsqu'une extension « policyQualifiers » est utilisée, celle-ci doit être précisée et traitée de la manière décrite dans les champs et le profil d'extension des LCR et des certificats X.509 de l'ICP du GC.

7.1.9 Traitement de la sémantique pour les extensions critiques de certificats

Les extensions critiques, lorsqu'elles sont précisées, doivent être interprétées de la manière décrite dans les champs et le profil d'extension des LCR et des certificats X.509 de l'ICP du GC.

7.2 Profil des LCR

7.2.1 Numéro de version

L'AC doit délivrer des LCR et des LCAR X.509 de version deux (2) ou de versions ultérieures si un tel emploi est approuvée par l'AGP de CANAFE. L'AC précisera dans son ÉPC les extensions utilisées que prennent en charge l'AC, ses AE et les entités finales.

7.2.2 Extensions des LCR et des entrées de LCR

Tous les logiciels d'ICP d'entités doivent traiter correctement toutes les extensions de LCR précisées dans les champs et le profil d'extension des LCR et des certificats X.509 de l'ICP du GC. L'AC précisera dans son ÉPC les extensions utilisées que prennent en charge l'AC, ses AE et les entités finales.

8. INSPECTION DE LA CONFORMITÉ ET AUTRES ÉVALUATIONS

Une inspection de la conformité permet de déterminer si les performances de l'AC satisfont aux exigences établies dans les présentes politiques de certification et l'ÉPC connexe.

Une inspection de conformité de l'AC sera menée selon les conditions établies par l'AGP de CANAFE. Les rapports d'inspection de la conformité ne seront pas rendus publics à moins que l'entente ou que la loi l'exige conformément à une autorisation judiciaire ou une exigence expresse de la loi ou d'une entente.

8.1 Fréquence ou circonstances de l'évaluation

L'AC fera mener une inspection de la conformité au moins une fois l'an.

Un inspecteur compétent à l'extérieur de l'AC mènera une (1) inspection sur cinq (5) de l'AC. L'AGP de CANAFE peut ordonner en tout temps la conduite d'une inspection de la conformité par un organisme de l'extérieur de l'AC.

L'AC certifiera annuellement à l'AGP de CANAFE qu'elle s'est conformée aux exigences des présentes politiques de certification, et ce en tout temps lors de la période dont il est question. Par ailleurs, elle fournira des motifs dans les cas où elle ne s'est pas conformée à ces politiques et indiquera toute période de non-conformité.

8.2 Identité et compétences de l'évaluateur

L'inspecteur doit faire la preuve de sa compétence dans le domaine de l'inspection de la conformité et doit être familier avec les exigences que l'AGP de CANAFE impose pour la délivrance et la gestion des certificats soumis aux présentes politiques de certification.

8.3 Rapport entre l'évaluateur et l'entité évaluée

Un inspecteur doit être indépendant de l'AC sur les plans de la gestion ou de l'exploitation.

Un inspecteur de l'extérieur de CANAFE doit être indépendant de l'AC et, suivant le cas, doit se conformer aux dispositions présentées dans le Code régissant la conduite des titulaires de charge publique en ce qui concerne les conflits d'intérêt et l'après-mandat ou le Code régissant les conflits d'intérêt et l'après-mandat s'appliquant à la fonction publique.

8.4 Sujets traités dans l'évaluation

Au minimum, l'inspection de la conformité aura la portée suivante :

1) L'ÉPC décrit, en détails suffisants, les politiques et les pratiques techniques, procédurales et de personnel de l'AC voulues dans le cadre des présentes politiques de certification;
2) L'AC met en place ces pratiques et politiques techniques, procédurales et de personnel et s'y conforme;
3) Le gestionnaire de dépôt, les AE et les personnes responsables chez le client mettent en place les pratiques techniques, procédurales et de personnel définies par l'AC et s'y conforment.

L'AGP de CANAFE peut accroître la portée d'une inspection de la conformité selon des conditions qu'elle juge appropriées.

8.5 Mesures prises par suite de l'écart

Les résultats de l'inspection doivent être présentés à l'autorité d'accréditation de l'AC et à l'AGP de CANAFE. En cas d'irrégularités, l'AC doit soumettre un rapport à l'autorité d'accréditation et à l'AGP de CANAFE quant à toute mesure que prendra l'AC pour donner suite au rapport d'inspection.

8.6 Communication des résultats

Les renseignements d'une inspection doivent être considérés comme étant de nature délicate et ne doivent pas être divulgués à aucune autre fin que celle liée à l'inspection ou selon les dispositions prévues dans une entente ou par la loi conformément à une autorisation judiciaire ou à une exigence expresse de la loi.