POLITIQUES DE CERTIFICATION
SIGNATURES NUMÉRIQUES ET CONFIDENTIALITÉ

POUR
L'INFRASTRUCTURE À CLÉ PUBLIQUE
DU GOUVERNEMENT DU CANADA

id-gocpki-certpcy-confidentiality-rudimentaryAssurance ::=
id-gocpki-certpcy-conf-1

id-gocpki-certpcy-confidentiality-basicAssurance ::=
id-gocpki-certpcy-conf-2

id-gocpki-certpcy-confidentiality-mediumAssurance ::=
id-gocpki-certpcy-conf-3

id-gocpki-certpcy-confidentiality-highAssurance ::=
id-gocpki-certpcy-conf-4

id-gocpki-certpcy-digitalSignature-rudimentaryAssurance ::=
id-gocpki-certpcy-Sign-1

id-gocpki-certpcy-digitalSignature-basicAssurance ::=
id-gocpki-certpcy-Sign-2

id-gocpki-certpcy-digitalSignature-mediumAssurance ::=
id-gocpki-certpcy-Sign-3

id-gocpki-certpcy-digitalSignature-highAssurance ::=
id-gocpki-certpcy-Sign-4

Version 4.0

Le 3 avril 2006

CONTRÔLE DES VERSIONS DU DOCUMENT

VERSION	DATE	AUTEUR	COMMENTAIRES
4.0	3 avr 2006		Document ébauche approuvé et ressorti comme v4.0.

POLITIQUES DE CERTIFICATION DU GOUVERNEMENT DU CANADA
GUIDE D'INTERPRÉTATION

Le lecteur est prié de noter que le texte du présent document s'applique à chacune des dix politiques de certification distinctes lorsque aucune distinction n'est précisée au sujet d'un ou de plusieurs éléments d'une section de ce document.

Dans certains cas, des distinctions sont faites par niveau d'assurance, par type de politique ou par type d'algorithme. Ces distinctions figurent dans des encadrés et elles indiquent que des exigences différentes s'appliquent au niveau d'assurance, au type de politique ou au type d'algorithme, ce qui est signalé par le titre de l'encadré.

Certains éléments de la politique de certification peuvent contenir des encadrés et du texte. Le texte dans les encadrés s'applique uniquement au niveau d'assurance concerné. Le texte non encadré s'applique uniformément à tous les niveaux d'assurance sans distinction.

TABLE DES MATIÈRES

1. INTRODUCTION

1.1 Aperçu

Ce document définit huit politiques de certification (PC) pour l'émission de certificats de signature numérique et de confidentialité qui seront utilisés principalement par les ministères et organisations (« ministères ») du gouvernement du Canada (GC). Ces huit PC se composent de quatre politiques de certification de signatures numériques et quatre politiques de confidentialité aux niveaux d'assurance suivants :

- Rudimentaire
- De base
- Moyen
- Élevé

Ces quatre niveaux d'assurance constituent un ensemble de références qui facilitent l'interprétation des politiques à des fins de mise en œuvre. Les AC peuvent être régies par des politiques multiples entre lesquelles des correspondances peuvent être établies efficacement grâce à l'utilisation de ces références.

Les certificats émis en vertu des présentes politiques de certification doivent être utilisés aux fins du GC. Ils peuvent être délivrés à des employés du gouvernement du Canada, à des employés d'autres gouvernements ou organisations internationales, à des personnes ou à des organisations ayant des relations contractuelles avec le GC, à des personnes ou à des organisations à des fins reliées à des programmes pour lesquels il a été déterminé qu'il était approprié de délivrer des certificats dans le cadre de l'une ou l'autre des politiques de certification définies dans le présent document.

Deux types de certificats sont délivrés en vertu de ces politiques de certification. Le premier type est le « certificat d'entreprise », qui lie de façon sûre le détenteur ou le titulaire d'un certificat et ses clés publiques, et qui est géré dans une infrastructure à clé publique (ICP). Le deuxième type est le « certificat Web ». Les navigateurs commerciaux standard supportent l'utilisation des certificats Web, mais pas celle des certificats d'entreprise. Le gouvernement du Canada peut émettre des certificats Web, mais seulement au niveau d'assurance rudimentaire.

En ce qui concerne la certification croisée (également appelée cocertification ou certification réciproque) entre des autorités de certification du GC et des AC qui ne relèvent pas de celui-ci, les présentes politiques de certification reflètent les exigences spécifiques du GC à l'égard d'une autorité de certification relevant de ce dernier. Les autorités de certification hors GC constateront peut-être que certaines dispositions ne s'appliquent pas à leurs activités. Le fait que toutes les dispositions relevant des diverses politiques de certification ne sont pas identiques n'exclut pas la certification croisée entre les autorités de certification du GC et celles qui ne relèvent pas du GC.

Les politiques de signature numérique visent la gestion et l'utilisation des certificats contenant des clés publiques utilisées pour les services d'authentification, d'intégrité des données et de non-répudiation.

Les politiques de confidentialité visent la gestion et l'utilisation des certificats contenant des clés publiques utilisées aux fins de l'établissement des clés de chiffrement, y compris le transfert des clés. Les certificats émis en vertu de ces politiques sont appropriés pour assurer la protection de l'information.

À moins qu'elles ne soient utilisées conjointement avec d'autres mécanismes de sécurité et parades procédurales, ces politiques ne doivent pas être utilisées pour assurer la confidentialité de l'information classifiée. Elles ne doivent pas non plus être utilisées lorsque la loi l'interdit.

Les ministères et organismes peuvent avoir besoin d'information additionnelle, de preuves d'identité ou encore d'autorisations pour des fins d'inscription à un programme spécifique. L'émission d'un certificat de clé publique, en vertu de l'une ou l'autre de ces politiques, ne garantit nullement que l'abonné a droit aux avantages associés à quelque programme que ce soit du GC ou à une participation à celui-ci. Le GC peut, à sa discrétion, refuser d'émettre un certificat de clé publique, ou encore révoquer un tel certificat.

Le gouvernement du Canada décline toute responsabilité découlant de toute action ou inaction de la part d'une organisation désignée, de toute nature, découlant de tout délit, contrat ou toute autre forme de réclamation reliée à l'utilisation, la fourniture, l'octroi sous licence ou l'emploi avec confiance de certificats si l'organisation désignée demande l'émission de certificats à des détenteurs de certificats au sein d'une organisation désignée.

Au sein du gouvernement du Canada, la responsabilité financière de l'AC, à l'égard de tout montant adjugé, jugement ou règlement négocié, sera limitée à :

0 $ par montant adjugé, jugement ou règlement en vertu des politiques de certification d'assurance rudimentaire;

5 000 $ par montant adjugé, jugement ou règlement en vertu des politiques de certification d'assurance de base;

50 000 $ par montant adjugé, jugement ou règlement en vertu des politiques de certification d'assurance moyenne;

1 000 000 $ par montant adjugé, jugement ou règlement en vertu des politiques de certification d'assurance élevée.

Le gouvernement du Canada décline toute responsabilité à l'égard de toute utilisation des certificats émis en vertu des politiques de certification au niveau d'assurance rudimentaire.

Ces limites ne s'appliquent pas aux organisations désignées ou aux personnes responsables désignées ou aux ministères et organisations qui peuvent prendre en charge les fonctions d'une autorité d'enregistrement (AE). Il incombe au gestionnaire opérationnel de programme (GOP) concerné d'établir toute limite de responsabilité pour le gouvernement du Canada à l'égard d'un programme.

La maintenance des systèmes ou des facteurs échappant au contrôle de l'AC peuvent influer sur la disponibilité des services offerts par l'AC. Le gouvernement du Canada décline toute responsabilité de quelque nature que ce soit à l'égard des facteurs qui échappent à son contrôle, y compris la disponibilité ou le bon fonctionnement d'Internet, des systèmes de télécommunications ou des autres infrastructures. Toute utilisation du terme « assurance » dans le présent document ne constitue nullement une représentation de garantie quant à la disponibilité de ces services.

Les certificats émis en vertu des présentes politiques de certification visent les types suivants de transactions auxquelles participe le GC :

- Publication d'information;
- Libre-service par les particuliers et les entreprises;
- Présentation de formulaires;
- Correspondance;
- Gestion des flux de documents dans les applications;
- Commerce électronique.

À la suite d'une évaluation des risques, les ministères demanderont à l'autorité de certification (AC) de délivrer des certificats à un ou plusieurs des quatre niveaux d'assurance spécifiés dans les présentes politiques de certification.

Les ministères et les propriétaires responsables d'application (PRA), avec l'aide des responsables de la sécurité du ministère, doivent choisir la politique de certification appropriée pour leurs applications et déterminer si on délivrera des paires de clés et des certificats de confidentialité et de signature numérique, ou l'un ou l'autre seulement. Les quatre niveaux d'assurance sont décrits en termes de leur adéquation ou de leur applicabilité générale dans le tableau ci-après.

NIVEAU D'ASSURANCE	EXIGENCES
Assurance rudimentaire	L'utilisation des clés de confidentialité au niveau d'assurance rudimentaire n'est pas appropriée pour assurer la confidentialité de l'information protégée. L'utilisation des clés de signature numérique au niveau d'assurance rudimentaire n'est pas appropriée lorsqu'une signature électronique est requise. Les certificats peuvent être émis en vertu de cette politique sans authentification de l'identité de l'abonné.
Assurance de base	L'utilisation des clés de confidentialité au niveau d'assurance de base est appropriée pour préserver la confidentialité d'information protégée qui, si elle était compromise, pourrait entraîner des dommages à l'extérieur de l'intérêt national. La politique du gouvernement sur la sécurité identifie ce type d'information comme étant classifiée PROTÉGÉ A.
Assurance moyenne	L'utilisation des clés de confidentialité au niveau d'assurance moyen est appropriée pour préserver la confidentialité d'information protégée qui, si elle était compromise, pourrait entraîner des dommages graves à l'extérieur de l'intérêt national. La politique du gouvernement sur la sécurité identifie ce type d'information comme étant classifiée PROTÉGÉ B.
Assurance élevée	L'utilisation des clés de confidentialité au niveau d'assurance élevé est appropriée pour préserver la confidentialité d'information protégée qui, si elle était compromise, pourrait entraîner des dommages extrêmement graves à l'extérieur de l'intérêt national. La politique du gouvernement sur la sécurité identifie ce type d'information comme étant classifiée PROTÉGÉ C.

1.2 Identification des politiques

NIVEAU D'ASSURANCE		SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance rudimentaire	**Nom de la politique**	Politique de certification de niveau d'assurance rudimentaire des signatures numériques pour l'ICP du GC	Politique de certification de niveau d'assurance rudimentaire de la confidentialité pour l'ICP du GC
	OID numérique	2.16.124.101.8.5.1.2.1.4	2.16.124.101.8.5.1.1.1.4
Assurance de base	**Nom de la politique**	Politique de certification de niveau d'assurance de base des signatures numériques pour l'ICP du GC	Politique de certification de niveau d'assurance de base de la confidentialité pour l'ICP du GC
	OID numérique	2.16.124.101.8.5.1.2.2.4	2.16.124.101.8.5.1.1.2.4

NIVEAU D'ASSURANCE		SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance moyenne	**Nom de la politique**	Politique de certification de niveau d'assurance moyen des signatures numériques pour l'ICP du GC	Politique de certification de niveau d'assurance moyen de la confidentialité pour l'ICP du GC
	OID numérique	2.16.124.101.8.5.1.2.3.4	2.16.124.101.8.5.1.1.3.4
Assurance élevée	**Nom de la politique**	Politique de certification de niveau d'assurance élevé des signatures numériques pour l'ICP du GC	Politique de certification de niveau d'assurance élevé de la confidentialité pour l'ICP du GC
	OID numérique	2.16.124.101.8.5.1.2.4.4	2.16.124.101.8.5.1.1.4.4

1.3 Participants à l'ICP

Les présentes politiques de certification soutiennent la communauté de l'ICP telle que définie dans les sous-sections suivantes.

1.3.1 Autorité de certification

Une AC doit :

1. appliquer les politiques de certification choisies ou définies pour son utilisation;
2. élaborer un énoncé des pratiques de certification (ECP), en conformité avec les présentes politiques de certification, afin de documenter la conformité de l'AC aux politiques de certification et aux autres exigences;
3. actualiser l'EPC selon les besoins;
4. superviser le personnel de l'AC qui accomplit des fonctions de l'AC conformément à l'EPC.

En ce qui concerne l'exploitation des serveurs de l'AC, il convient de mentionner les rôles importants suivants :

1. L'**utilisateur maître de l'ICP** est responsable de configurer et de maintenir le matériel et les logiciels du système de l'AC; de lancer et de terminer les services de l'AC; de procéder à la création initiale des comptes des responsables de la sécurité de l'ICP.
2. Le **responsable de la sécurité de l'ICP** est responsable de gérer les administrateurs de l'ICP et les autres responsables de la sécurité de l'ICP et de configurer les politiques de sécurité de l'AC.
3. L'**administrateur de l'ICP** est responsable de gérer le processus d'initialisation des abonnés; de créer, renouveler ou révoquer les certificats; et de distribuer les jetons (le cas échéant).

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

Le service d'assistance de l'ICP est associé à l'AC; il est responsable de fournir une aide aux abonnés en ce qui concerne la délivrance, l'actualisation ou la révocation des certificats. Le service d'assistance de programme peut prendre en charge un certain nombre des fonctions qui sont dévolues au service d'assistance de l'ICP.

1.3.2 Autorités d'enregistrement

Une autorité d'enregistrement (AE) est une personne ou une organisation qui est chargée de vérifier l'identité d'un abonné. C'est l'AE qui amorce le processus de délivrance des certificats par

l'AC, mais ce n'est pas elle qui signe ou émet les certificats. L'AE peut utiliser un système dans lequel le processus d'identification peut être réalisé en ligne, et elle peut accomplir d'autres tâches à la demande de l'AC. Une autorité locale d'enregistrement (ALE) est associée à une organisation spécifique, et elle dispose de l'autorité voulue pour vérifier l'identité et approuver les demandes à distance de l'AC.

L'AE vérifie l'autorisation de l'ALE d'agir pour le compte d'une organisation spécifique. La validation de l'autorité de ces personnes est décrite dans la section 3.2.5.

1.3.3 Abonnés

Un abonné est une entité qui s'inscrit auprès d'une AC pour obtenir un certificat à la suite d'un processus d'enregistrement. L'identité de l'abonné est vérifiée et authentifiée par l'ALE ou l'AE avant qu'un certificat lui soit délivré par l'AC. Le certificat résultant identifie le propriétaire du certificat dans le nom sujet qui reflète la liaison d'identité accomplie dans le processus d'approbation de la demande.

Un abonné peut être une entité à l'intérieur ou à l'extérieur du GC. Les employés du GC sont implicitement liés par les dispositions d'une politique d'utilisation acceptable. Les entités à l'extérieur du GC doivent signer ou convenir de respecter les termes d'une entente d'abonnement avant de se voir délivrer un certificat de clé publique signé par l'AC qui fonctionne dans le cadre des présentes politiques de certification.

Une personne peut demander un certificat destiné à être utilisé par elle-même ou pour le compte d'une autre entité, si elle dispose pour cela d'une autorisation vérifiable appropriée. Cette autre entité peut être une application, un appareil, un rôle organisationnel ou une autre personne.

C'est uniquement dans des circonstances exceptionnelles et avec l'autorisation de l'AC qu'une personne peut agir pour le compte d'une autre personne.

Organisations désignées

Une organisation désignée est une organisation qui assume toutes les responsabilités à l'égard des activités d'identification et d'authentification accomplies, ainsi que de toutes les utilisations de certificats émis sous sa responsabilité. À l'intérieur d'une organisation désignée, une personne responsable désignée (PRD) est autorisée à agir pour le compte de l'organisation dans la réalisation des fonctions de l'ALE. Le Ministère peut, à sa seule discrétion, déterminer si une organisation peut être une organisation désignée.

L'AC peut, à sa seule discrétion, refuser d'émettre des certificats en réponse aux demandes de certificat qui lui sont présentées.

1.3.4 Parties utilisatrices

Une partie utilisatrice est un destinataire d'un certificat qui agit en se fiant à ce dernier ou à une signature numérique vérifiée au moyen de ce certificat.

Une partie utilisatrice est soit :

(a) Un abonné de l'ICP du GC;

(b) Une personne ou une organisation qui a reçu un certificat numérique d'une AC qui a signé une entente de certification croisée avec l'ICP du GC, ou qui a conclu un autre type d'accord acceptable pour l'AGP de l'ICP du GC.

Les personnes ou organisations autres que celles qui sont mentionnées ci-dessus ne sont pas autorisées à se fier à des certificats émis par l'AC et, si elles le font, c'est à leurs propres risques. **Le gouvernement du Canada décline toute responsabilité qui peut découler d'un tel emploi.**

1.3.5 Autres participants

Autorité de gestion des politiques de l'ICP du GC

L'autorité de gestion des politiques (AGP) du GC est un comité interministériel composé de cadres supérieurs agissant pour le compte du GC pour gérer l'ICP du GC conformément à la « *Politique de gestion de l'infrastructure à clé publique du gouvernement du Canada* ».

L'AGP de l'ICP du GC est responsable de ce qui suit :

1. Approuver les présentes politiques de certification ainsi que les EPC à l'égard des AC communes conformément à la « *Politique de l'infrastructure à clé publique du gouvernement du Canada* »;
2. Recommander des ententes de certification croisée ou d'interopérabilité avec des domaines externes à l'AC;
3. Élaborer des politiques de certification types destinées à être utilisées par les AC des ministères;
4. Fournir une orientation politique à toutes les AC du GC.

L'AGP de l'ICP du GC relève du Secrétariat du Conseil du Trésor pour ce qui est de l'orientation et de la gestion de l'ICP du gouvernement du Canada.

Autorité d'accréditation (AA)

Le dirigeant principal de l'information (DPI) du GC est responsable de l'accréditation des AC communes conformément à la « *Politique de l'infrastructure à clé publique du gouvernement du Canada* ».

Gestionnaire de référentiels

Le gestionnaire de référentiels est une personne ou une organisation qui est responsable de tenir à jour un ou plusieurs :

1. Référentiels contenant des informations pertinentes comme des certificats et des listes de certificats révoqués;
2. Serveurs de vérification en ligne de l'état des certificats.

À chaque AC est associée au moins un référentiel de certificats et de LCR.

L'AC peut prendre en charge cette fonction elle-même, mais elle n'y est pas tenue. Lorsqu'un référentiel n'est pas contrôlé par l'AC, cette dernière doit établir les termes et les conditions de son association avec le gestionnaire du référentiel, et cette entente doit porter notamment sur les sujets suivants : disponibilité, contrôle d'accès, intégrité des données, protection des informations personnelles, réplication des annuaires, chaînage des annuaires et, le cas échéant, référencement d'annuaires.

Propriétaire responsable d'une application

Le propriétaire responsable d'une application (PRA) est une personne dans un ministère ou un organisme qui est responsable de la gestion d'une application particulière (par exemple le système de courrier électronique du ministère), d'un programme (par exemple la sécurité), d'un programme particulier ou d'une activité horizontale qui englobe plusieurs ministères ou organismes.

Un PRA peut être :

1. Un dirigeant principal de l'information;

2. Un directeur de la technologie de l'information;
3. Un directeur de la gestion de l'information;
4. Un gestionnaire opérationnel de programme;
5. Un responsable de la sécurité du ministère;
6. Une personne quelconque qui assume les responsabilités d'un PRA telles qu'elles sont définies ci-dessus.

Le PRA est responsable des exigences qui régissent l'inscription dans le programme concerné, et il peut imposer des exigences supplémentaires en plus de celles qui sont stipulées par la politique.

Le PRA, avec l'aide des responsables de la sécurité du ministère, doit déterminer les politiques de certification qui sont appropriées pour ses applications, et notamment si ces clients se verront émettre des certificats et des paires de clés de signature numérique et de confidentialité, ou seulement un des deux types.

Dans les ministères et les organismes, ce sont les services d'assistance des divers programmes qui sont responsables de fournir une aide aux abonnés en ce qui concerne les applications de ces programmes. Cette fonction est distincte du service d'assistance de l'ICP, qui est concerné par les problèmes spécifiquement associés aux certificats et aux clés publiques. Un service d'assistance de programme peut accomplir certaines fonctions du service d'assistance de l'ICP.

1.4 Utilisation des certificats

1.4.1 Utilisations appropriées des certificats

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance rudimentaire	Cette politique permet d'assurer l'intégrité et l'authentification des transactions ou des communications du gouvernement du Canada, mais non pour assurer l'authentification de l'identité. Les signatures numériques générées au moyen de clés de signature privées créées en vertu de cette politique ne sont pas destinées à servir de signatures pour des transactions ou communications exigeant des signatures.	Cette politique s'applique à des utilisations reliées aux certificats comme l'établissement d'une clé de chiffrement. Elle n'est pas jugée appropriée pour protéger la confidentialité des informations désignées.
Assurance de base	Cette politique permet d'assurer l'intégrité et l'authentification des transactions opérationnelles du gouvernement du Canada qui, si elles étaient falsifiées, pourraient causer des pertes financières mineures ou dont la correction pourrait exiger seulement un recours légal, et elles soutiennent la non-répudiation.	Cette politique s'applique à des utilisations des certificats comme l'établissement de clés de confidentialité pour de l'information qui, si elle était compromise, pourrait causer des dommages à l'extérieur de l'intérêt national. La politique du gouvernement sur la sécurité identifie ce type d'information comme était de

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
	Cette politique permet d'authentifier l'identité du titulaire du certificat.	niveau PROTÉGÉ A. Même combinés à d'autres mécanismes de sécurité appropriés, ces certificats ne doivent pas être utilisés pour la protection d'informations classifiées.
Assurance moyenne	Cette politique permet d'assurer l'intégrité et l'authentification des transactions opérationnelles du gouvernement du Canada qui, si elles étaient falsifiées, pourraient causer des dommages à la propriété, des blessures corporelles, des pertes financières importantes ou dont la correction pourrait exiger un recours légal, et elles soutiennent la non-répudiation. Cette politique permet d'authentifier l'identité du titulaire du certificat.	Cette politique s'applique à des utilisations des certificats comme l'établissement de clés de confidentialité pour de l'information qui, si elle était compromise, pourrait causer des dommages sérieux à l'extérieur de l'intérêt national. La politique du gouvernement sur la sécurité identifie ce type d'information comme étant de niveau PROTÉGÉ B.
Assurance élevée	Cette politique permet d'assurer l'intégrité et l'authentification des transactions opérationnelles du gouvernement du Canada qui, si elles étaient falsifiées, pourraient causer des pertes de vie, des emprisonnements, des pertes financières majeures ou dont la correction pourrait exiger un recours légal, et elles soutiennent la non-répudiation.	Cette politique s'applique à des utilisations des certificats comme l'établissement de clés de confidentialité pour de l'information qui, si elle était compromise, pourrait causer des dommages extrêmement sérieux à l'extérieur de l'intérêt national. La politique du gouvernement sur la sécurité identifie ce type d'information comme étant de niveau PROTÉGÉ C.

Compte tenu de toute exigence législative ou réglementaire applicable à un programme et des résultats d'une évaluation des risques et des menaces touchant une application, les certificats peuvent être utilisés dans des applications aux fins suivantes :

- Publication d'information;
- Libre-service par des particuliers et des entreprises;
- Présentation de formulaires;
- Correspondance;
- Gestion des flux de travaux dans les applications;
- Commerce électronique.

Les certificats peuvent aussi être utilisés pour satisfaire d'autres besoins généraux ou spécifiques du GC.

Bien qu'il soit permis d'échanger (en importation ou en exportation) des certificats à des fins officielles du GC avec des entités qui ne sont pas des parties utilisatrices telles qu'elles sont définies dans la section 1.3.4 du présent document, ces certificats doivent être utilisés seulement pour assurer la confidentialité de l'information, jusqu'au niveau d'assurance pour lequel ils ont été émis, le niveau d'assurance moyen inclusivement.

1.4.2 Utilisations interdites des certificats

NIVEAU D'ASSURANCE	EXIGENCES
Assurance rudimentaire **Assurance de base**	Les certificats émis par l'AC ne doivent pas être utilisés pour : 1. Une application devant fonctionner sans défaillance, y compris celles qui sont associées aux systèmes suivants notamment : (a) Exploitation d'installations nucléaires; (b) Systèmes de contrôle de la circulation aérienne; (c) Systèmes de navigation aérienne; (d) Systèmes de maintien des fonctions vitales dans les hôpitaux; (e) Stations municipales de traitement de l'eau; (f) Systèmes de conduite d'armes; (g) Tout autre système dont la défaillance pourrait causer des blessures, la mort, des dommages à la propriété ou à l'environnement. 2. Les transactions pour lesquelles les lois applicables interdisent l'utilisation des signatures numériques, ou lorsque cela est interdit par la loi de quelque autre façon; 3. La protection des informations classifiées.
Assurance moyenne **Assurance élevée**	Les certificats émis par l'AC ne doivent pas être utilisés pour : 1. Les transactions pour lesquelles les lois applicables interdisent l'utilisation des signatures numériques, ou lorsque cela est interdit par la loi de quelque autre façon; 2. La protection des informations classifiées, à moins d'avoir recours en appoint à d'autres mécanismes de sécurité et parades procédurales additionnelles.

Bien qu'il soit permis d'échanger (en importation ou en exportation) des certificats à des fins officielles du GC avec des entités qui ne sont pas des parties utilisatrices telles qu'elles sont définies dans la section 1.3.6 du présent document, ces certificats ne doivent pas être utilisés à des fins de signature numérique ou pour assurer la confidentialité d'informations de niveau PROTÉGÉ C ou classifiées.

1.5 Administration des politiques

1.5.1 Organisation responsable de l'administration du document

L'autorité de gestion des politiques (AGP) de l'ICP du GC, qui relève du Secrétariat du Conseil du Trésor, Ottawa (Canada), est responsable des présentes politiques de certification.

1.5.2 Personne à contacter

Présidence, Autorité de gestion des politiques de l'ICP du gouvernement du Canada
Travaux publics et Services gouvernementaux Canada
2745, rue Iris, 6e étage
Ottawa (Ontario), Canada
K1A 0R5
Courriel : pki@pwgsc.gc.ca

1.5.3 Personne qui détermine l'adéquation de l'EPC à la politique

Le Comité consultatif de l'autorité de gestion des politiques (CAP) fournit des avis et des conseils à l'AGP en ce qui concerne l'adéquation des politiques et des procédures.

L'AGP de l'ICP du GC est responsable d'approuver les politiques de certification ainsi que l'énoncé des pratiques de certification pour les AC communes, conformément à la « *Politique de l'infrastructure à clé publique du gouvernement du Canada* ».

1.5.4 Procédures d'approbation de l'EPC

Après avoir déterminé que l'EPC établit de façon satisfaisante la manière dont l'AC mettra en œuvre les exigences des présentes politiques de certification, l'AGP de l'ICP du GC, conformément à la section 1.3.5, approuvera l'EPC associé aux présentes politiques de certification ainsi qu'à leurs modifications le cas échéant.

1.6 Définitions et sigles

1.6.1 Définitions générales

Expression	Définition
Autorité d'accréditation	Entité de gestion habilitée à permettre à une entité de l'ICP de fonctionner dans les limites d'un domaine donné et d'accepter les risques résiduels associés. Le DPI du gouvernement du Canada est responsable de l'accréditation des AC communes conformément à la « *Politique de l'infrastructure à clé publique du gouvernement du Canada* ».
Données d'activation	Données privées, autres que les clés, requises pour accéder aux environnements de sécurité personnels qui doivent être protégés (par exemple mot de passe).
Propriétaire responsable de l'application	Personne au sein d'un ministère ou d'un organisme qui est responsable de la gestion d'une application particulière (par exemple la messagerie du ministère), d'un programme (par exemple la sécurité), d'un programme particulier ou d'une activité horizontale qui englobe plusieurs ministères ou organismes.
Liste des autorités révoquées	Liste des certificats d'AC révoqués. Une LAR est une liste de certificats révoqués. Ces certificats sont des certificats croisés d'AC ou des certificats autosignés.
Pont de l'ICP fédérale du Canada	L'autorité de certification du pont de l'ICP du gouvernement du Canada. Sous la direction de l'Autorité de gestion des politiques de l'ICP du GC, le PIFC signe et gère les certificats croisés avec les AC de niveau supérieur du GC ainsi qu'avec les AC qui ne relèvent pas du GC. Il ne gère pas les certificats d'abonné.
Certificat	Fichier électronique dans un format conforme à la recommandation X.509 de l'UIT-T qui contient la clé publique d'un abonné ainsi que des informations connexes, signé numériquement au moyen de la clé privée de l'autorité de certification qui l'a délivré.

Expression	Définition
Liste des certificats révoqués	Liste publiée et actualisée par l'autorité de certification, sur laquelle figurent les certificats qui ont été révoqués avant leur délai prévu d'expiration.
Autorité de vérification de l'état des certificats	Entité fiable offrant en ligne aux parties utilisatrices des services de vérification de la validité des certificats et qui peut également fournir des renseignements additionnels sur les attributs du certificat.
Autorité de certification	Entité de confiance reconnue par une ou plusieurs entités finales, pour l'émission et la gestion des certificats de clé publique X.509 et des LCR. Chacune des AC au sein de l'ICP du GC peut émettre des certificats en vertu de politiques choisies en fonction du niveau d'assurance pour lequel l'AC a été accréditée.
Logiciel de l'autorité de certification	Logiciel qui gère la clé de signature de l'AC, le cycle de vie des certificats et les LCR, ainsi que les paires de clés des entités finales.
Énoncé des pratiques de certification	Énoncé des pratiques qu'applique une autorité de certification aux fins d'émettre des certificats. L'EPC doit contenir ou indiquer les autres sources qui contiennent suffisamment d'information pour démontrer à l'AGP concernée la manière dont il satisfait aux exigences contenues dans la ou les PC.
Chaîne de validation des certificats	Chaîne de certificats débutant par le certificat d'un détenteur de clé publique (une entité) signé par une AC – le certificat de l'AC de l'entité – et un ou plusieurs certificats additionnels d'AC signés par d'autres AC. Si l'utilisateur de la clé publique (la partie utilisatrice) ne possède pas déjà une copie assurée de la clé publique de l'AC qui a signé le certificat de l'entité, le nom de l'AC et les informations connexes (par exemple la période de validité ou les contraintes relatives aux noms), il peut alors s'avérer nécessaire d'avoir un certificat additionnel pour obtenir cette clé publique, aux fins de vérification. Souvent, il peut s'avérer nécessaire d'avoir une chaîne de certificats multiples. Ces chaînes sont appelées des chemins de certification.
Gestion de la configuration	Processus d'identification et de définition des éléments critiques d'un système, ainsi que de contrôle de tout changement apporté à ces éléments au cours de leur cycle de vie.
Certificat croisé ou cocertificat	Certificat émis par une autorité de certification afin d'établir un lien de confiance entre elle et une autre autorité de certification.
Gardien	Personne qui présente une demande de certificat pour le compte d'un appareil ou d'une application et qui est responsable des activités de gestion du certificat qui requièrent une intervention humaine. Sur acceptation du certificat émis, les obligations de l'abonné s'étendent au gardien du certificat.
Intégrité des données	Cette expression désigne, quand on utilise des signatures numériques, l'assurance que les données ne sont pas modifiées à partir du moment où la signature numérique est appliquée aux données. Il existe d'autres moyens d'assurer l'intégrité des données, notamment l'utilisation de codes d'authentification des messages.
Organisation désignée	Organisation qui est autorisée à nommer une ALE pour l'enregistrement des personnes, des appareils, des applications ou des rôles à l'intérieur de cette organisation, et qui assume toutes les responsabilités à l'égard des activités d'identification et d'authentification accomplies ainsi que de toutes les utilisations des certificats délivrés sous son autorité.

Expression	Définition
Personne responsable désignée	Personne à l'intérieur d'une organisation désignée qui est autorisée par celle-ci à la représenter et à agir pour le compte de l'organisation aux fins des demandes de délivrance de certificats.
Ministère ou organisme	Ministères énumérés aux annexes I, I.1 et II de la *Loi sur la gestion des finances publiques* (LGFP) et a) Toute commission exigée par la *Loi sur les enquêtes*, désignée par décret du gouverneur en conseil comme étant un ministère aux fins de la LGFP; b) Les Forces canadiennes; c) Les organismes ou sociétés d'État qui ont conclu des accords ou des ententes avec le Secrétariat du Conseil du Trésor afin d'adopter les exigences des présentes politiques de certification et de les appliquer dans leurs organisations.
Parrain ministériel	Personne ou organisation au sein d'un ministère à qui est confiée la tâche de diriger la délivrance des certificats. Un parrain ministériel peut être un gestionnaire opérationnel de programme, un responsable de la sécurité du ministère, un gestionnaire ou un superviseur.
Signature numérique	Résultat de la transformation des données au moyen d'un système cryptographique utilisant des clés, de sorte que la personne qui reçoit les données initiales peut déterminer si : a) la transformation a été réalisée à l'aide de la clé qui correspond à la clé du signataire; b) les données ont été modifiées depuis cette transformation.
Entité finale	Entité qui utilise les clés et les certificats créés dans une infrastructure à clé publique à des fins autres que la gestion proprement dite des clés et des certificats. Une entité finale peut être un abonné, une partie utilisatrice, un appareil, un rôle ou une application qui utilise un certificat qui lui a été attribué.
Enregistrement	Processus par lequel une personne s'inscrit pour recevoir des services d'un programme spécifique ou effectuer des transactions avec celui-ci.
Certificat d'entreprise	Certificat émis par une AC et destiné à être utilisé par des personnes, des rôles, des appareils ou des applications. Ces certificats sont entièrement gérés dans le cadre d'une ICP et ils peuvent faire l'objet : a) d'une vérification automatique de la révocation; b) d'une mise à jour transparente des justificatifs; c) d'une mise à jour dynamique et transparente de la politique de sécurité. Un certificat d'entreprise associe d'une manière sûre le propriétaire du certificat à ses clés publiques. Les navigateurs commerciaux standard ne supportent pas les certificats d'entreprise.
Entité	Élément autonome de l'ICP. Il peut s'agir d'une AC, d'un rôle de confiance à l'intérieur d'une AC, d'une AE ou d'une entité finale.
Sans défaillance	Cette expression désigne l'organisation des programmes ou des systèmes de traitement afin d'assurer la sécurité ou de leur permettre d'accomplir leur mission assignée quand la défaillance d'un matériel ou d'un logiciel est détectée dans un programme ou un système.
Sécurité intégrée	Cette expression désigne l'organisation des programmes ou des systèmes de traitement d'une telle manière que leur sécurité soit préservée quand la

Expression	Définition
	défaillance d'un matériel ou d'un logiciel est détectée dans un programme ou un système.
Autorité de gestion des politiques de l'ICP du GC	L'Autorité de gestion des politiques du gouvernement du Canada est un comité interministériel composé de cadres supérieurs du GC. L'AGP de l'ICP du GC relève du Secrétariat du Conseil du Trésor pour ce qui est de l'orientation et de la gestion de l'infrastructure à clé publique du gouvernement du Canada
Zone de haute sécurité	Une zone de haute sécurité est une zone dont l'accès est contrôlé au moyen d'un point d'accès; seuls ont accès à cette zone (1) les personnels autorisés qui possèdent la cote de sécurité nécessaire; (2) les visiteurs autorisés et accompagnés de la façon appropriée. L'accès à une zone de haute sécurité doit être possible uniquement à partir d'une zone de sécurité et elle doit être séparée de cette dernière et des zones de travail au moyen d'un périmètre possédant les caractéristiques recommandées dans l'EMR. Les zones de haute sécurité sont surveillées 24 heures par jour, sept jours par semaine, par des gardiens de sécurité, par d'autres personnels ou par des moyens électroniques.
Personne	Particulier, à l'opposé d'un groupe, d'une classe ou de tout autre type d'organisation.
Données d'initialisation	Codes ou autres données utilisés par un abonné pour générer une clé de signature numérique privée et obtenir des certificats de clé publique de l'AC (par exemple un numéro de référence et un code d'authentification).
Autorité locale d'enregistrement	Fonction d'enregistrement des certificats du processus de vérification de l'identité et d'approbation des demandes, propre à un groupe local spécifique. À l'intérieur d'une organisation cliente, la personne responsable désignée (PRD) et le parrain ministériel sont autorisés à accomplir les fonctions de l'ALE dans l'organisation cliente ou le ministère respectivement.
Non-répudiation	Dans un contexte juridique, la non-répudiation signifie qu'il y a suffisamment de preuves pour persuader un arbitre de l'origine et de l'intégrité de données numériquement signées, malgré toute dénégation par l'expéditeur présumé. Dans un contexte technique, la non-répudiation désigne l'assurance qu'une partie utilisatrice a que si une clé publique de vérification est utilisée pour valider une signature numérique, cette signature a été faite avec la clé privée de signature correspondante.
Identificateur d'objet	Identificateur alphanumérique/numérique unique, enregistré conformément à la norme d'enregistrement de l'ISO pour désigner un objet ou une classe d'objets spécifique.
Zone de travail	Une zone de travail est une zone dont l'accès est restreint au personnel qui y travaille et aux visiteurs adéquatement accompagnés. Les zones de travail doivent être surveillées au moins périodiquement, en fonction d'une évaluation des menaces et des risques (EMR), et elles doivent de préférence être accessibles depuis une zone d'accueil.
Organisation	Administration, organisme, société, partenariat, trust, entreprise conjointe ou autre association. Une organisation peut également être une entreprise ayant un seul propriétaire, si elle est ainsi reconnue.
Environnement de sécurité personnel	Zone de stockage sécurisée contenant de l'information comme les clés privées et les certificats connexes. La zone de stockage est chiffrée et protégée par des moyens cryptographiques. Il existe plusieurs formes de stockage, allant des fichiers aux jetons cryptographiques infalsifiables.

Expression	Définition
Infrastructure à clé publique	Ensemble de politiques, processus, plates-formes de serveur, logiciels et postes de travail, utilisés pour gérer des certificats et des clés.
Administrateur de l'ICP	Personne responsable : (a) de la gestion du processus d'initialisation des abonnés; (b) de la création, du renouvellement ou de la révocation des certificats; (c) de la distribution des jetons (le cas échéant).
Utilisateur maître de l'ICP	Personne responsable : (a) de la configuration et de la maintenance du matériel et du logiciel du système de l'AC; (b) du lancement et de la cessation des services de l'AC; (c) de la création initiale des comptes des responsables de la sécurité de l'ICP.
Responsable de la sécurité de l'ICP	Personne responsable de gérer les administrateurs de l'ICP et les autres responsables de la sécurité de l'ICP, ainsi que de configurer les politiques de sécurité de l'AC.
Programme	Ensemble spécifique de services gouvernementaux offerts par des moyens électroniques.
Gestionnaire opérationnel du programme	Personne qui, au sein d'un ministère ou d'un organisme, est responsable de gérer un programme particulier du gouvernement du Canada.
Zone d'accueil	Zone située à l'entrée de l'édifice où se fait le contact initial entre le public et le ministère, où l'on offre des services et des renseignements et à partir d'où l'accès aux zones restreintes est contrôlé. La surveillance s'y fait à divers degrés par le personnel y travaillant, par les autres employés ou par le personnel de la sécurité. L'accès par le public peut être limité à certaines heures de la journée ou pour des raisons déterminées.
Autorité d'enregistrement	Personne responsable de l'identification et de l'authentification des abonnés et des autres entités finales, mais qui ne signe pas ou n'émet pas de certificats. L'AC peut demander à l'AE d'exécuter certaines tâches.
Partie utilisatrice	Destinataire d'un certificat qui agit en se fiant à ce dernier ou à toute signature numérique vérifiée au moyen du certificat.
Référentiel	Système dans lequel les LCR, les LAR ainsi que les certificats de clé publique sont stockés pour y être consultés par les entités. Un annuaire X.500 constitue un exemple de référentiel.
Gestionnaire de référentiel	Personne ou rôle responsable de tenir à jour un ou plusieurs : a) référentiels contenant des informations pertinentes comme des certificats et des listes de certificats révoqués; b) serveurs de vérification en ligne de l'état des certificats.
Titulaire d'un rôle	Personne qui représente un rôle à l'égard duquel un certificat a été délivré et qui est responsable des activités de gestion du certificat qui nécessitent l'intervention humaine. Sur réception du certificat délivré à l'égard du rôle, les obligations de l'abonné s'étendent au titulaire du rôle.
Zone de sécurité	Zone dont l'accès est restreint au personnel autorisé ainsi qu'aux visiteurs autorisés et adéquatement accompagnés. Une zone de sécurité est surveillée 24 heures par jour, sept jours par semaine, par le personnel de sécurité, d'autres personnels ou des moyens électroniques
Stockage	Processus consistant à stocker les clés de signature privée et les clés de confidentialité privée dans des profils sur des serveurs exploités par l'AC. Quand les abonnés désirent utiliser leurs clés, ils accèdent à leur profil en utilisant leur nom d'utilisateur et leur mot de passe, qu'ils sont les seuls à connaître. Ils récupèrent leur profil chiffré via un tunnel SSL (Secure Sockets Layer) et, après avoir été utilisée, la copie locale du profil est

Expression	Définition
	détruite. Un abonné peut également stocker son profil localement. En tout temps, le profil est sous le contrôle exclusif de l'abonné.
Abonné	Entité qui s'inscrit auprès d'une AC pour obtenir un certificat à la suite d'un processus d'enregistrement et d'approbation. Avant qu'un certificat lui soit délivré, l'abonné doit tout d'abord signer un contrat qui comporte les dispositions d'une entente d'abonnement, ou une entente d'abonnement proprement dite, ou encore il doit accepter de se conformer aux conditions d'une entente d'abonnement. À l'intérieur du GC, les employés doivent s'engager à respecter les conditions de la politique sur les utilisations acceptables.
Certificat Web	Certificat délivré à des utilisateurs (par exemple des clients et des serveurs) par une AC, et qui lie de façon sûre le propriétaire du certificat à ses clés publiques. Une clé racine pour l'AC est en général intégrée dans les navigateurs commerciaux, ce qui permet la vérification de ces certificats Web.

1.6.2 Sigles

SIGLE ANGLAIS	EXPRESSION ANGLAISE	EXPRESSION FRANÇAISE	SIGLE FRANÇAIS
AA	Accreditation Authority	Autorité d'accréditation	AA
ARL	Authority Revocation List	Liste des autorités révoquées	LAR
ARO	Application Responsible Owner	Propriétaire responsable de l'application	PRA
CA	Certification Authority	Autorité de certification	AC
CFPB	Canadian Federal PKI Bridge	Pont de l'ICP fédérale canadienne	PIFC
CIO	Chief Information Officer	Dirigeant principal de l'information	DPI
CP	Certificate Policy	Politique de certification	PC
CPS	Certification Practice Statement	Énoncé des pratiques de certification	EPC
CRL	Certificate Revocation List	Liste des certificats révoqués	LCR
CSE	Communications Security Establishment	Centre de la sécurité des télécommunications	CST
DES	Data Encryption Standard	Data Encryption Standard	DES
DN	Distinguished Name	Nom distinctif	DN
DRI	Designated Responsible Individual	Personne responsable désignée	PRD
ERC	Enhanced Reliability Check	Vérification approfondie de la fiabilité	VAF
FIPS	Federal Information Processing Standards	Federal Information Processing Standards	FIPS
GoC	Government of Canada	Gouvernement du Canada	GC
GOL	Government of Canada On-Line	Gouvernement du Canada en direct	GED
GSP	Government Security Policy	Politique du gouvernement sur la sécurité	PGS
I&A	Identification et authentification	Identification et authentification	I&A
ITU	International Telecommunications Union	Union internationale des télécommunications	UIT
LRA	Local Registration Authority	Autorité locale d'enregistrement	ALE
OCSP	Online Certificate Status Protocol	Online Certificate Status Protocol	OCSP
OID	Object Identifier	Identificateur d'objet	OID

SIGLE ANGLAIS	EXPRESSION ANGLAISE	EXPRESSION FRANÇAISE	SIGLE FRANÇAIS
PAC	Policy Management Authority Advisory Committee	Comité consultatif de l'autorité de gestion des politiques	CAP
PBM	Program Business Manager	Gestionnaire opérationnel de programme	GOP
PIA	Privacy Impact Assessment	Évaluation des facteurs relatifs à la vie privée	EFVP
PKI	Public Key Infrastructure	Infrastructure à clé publique	ICP
PMA	Policy Management Authority	Autorité de gestion des politiques	AGP
PSE	Personal Security Environment	Environnement de sécurité personnel	ESP
RA	Registration Authority	Autorité d'enregistrement	AE
RDN	Relative Distinguished Name	Nom distinctif relatif	NDR
RSA	Rivest-Shamir-Adleman	Rivest-Shamir-Adleman	RSA
SHA-1	Secure Hash Algorithm –1	Secure Hash Algorithm –1	SHA-1
SSL	Secure Sockets Layer	Secure Sockets Layer	SSL
TBS	Treasury Board of Canada Secretariat	Secrétariat du Conseil du Trésor	SCT
TRA	Threat and Risk Assessment	Évaluation des menaces et des risques	EMR
URL	Uniform Resource Locator	Adresse URL	URL

2. RESPONSABILITÉS CONCERNANT LA PUBLICATION ET LES RÉFÉRENTIELS

2.1 Référentiels

L'AC possédera au moins un référentiel de certificats et de LCR qui lui soit associé.

L'AC peut, mais elle n'y est pas tenue, prendre en charge cette fonction elle-même. Lorsqu'un référentiel n'est pas sous le contrôle de l'AC, l'AC doit établir les termes et les conditions de son association avec le gestionnaire de référentiel, qui doivent porter notamment sur les sujets suivants : disponibilité, contrôle d'accès, intégrité des données, protection des informations personnelles, réplication des annuaires, chaînage des annuaires et, le cas échéant, référencement des annuaires.

2.2 Publication des informations sur les certificats

Lorsque l'AC exploite un référentiel ou agit à titre de gestionnaire de référentiel, elle doit :

1. publier les certificats et les LCR;
2. indiquer aux abonnés l'adresse des serveurs de LCR ou OCSP;
3. publier l'état des certificats dans les listes de révocation des certificats, les serveurs OCSP ou autrement rendre cette information disponible à l'intérieur des délais spécifiés dans les présentes politiques de certification.

En ce qui concerne les politiques et les pratiques, l'AC doit :

1. fournir aux abonnés et aux parties utilisatrices l'adresse d'un site Web;
2. publier sa PC, signée numériquement par un représentant autorisé de l'AC, sur le site Web évoqué ci-dessus;
3. avertir, ou demander aux ministères d'avertir, les abonnés et les parties utilisatrices de tout changement concernant leurs droits, privilèges et obligations concernant les certificats;
4. à sa discrétion, fournir aux parties concernées, aux termes et conditions qu'elle juge appropriées, tout ou partie de l'EPC, à des fins d'audit, d'inspection, d'accréditation ou de certification croisée.

2.3 Moment ou fréquence de la publication

Aucune exigence n'est stipulée.

2.4 Contrôles accès aux référentiels

L'AC doit imposer des contrôles d'accès aux référentiels en ce qui concerne les certificats, les LCR ou la vérification en ligne de l'état des certificats.

L'AC doit configurer le système d'exploitation et les contrôles d'accès aux référentiels de façon que seul le personnel autorisé de l'AC puisse écrire dans la version en ligne de la PC ou la modifier.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1 Noms

3.1.1 Types de noms

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire **Assurance de base** **Assurance moyenne** **Assurance élevée**	Chaque entité : a) doit posséder un nom distinctif (DN) X.501 unique et clairement distinct, dans le champ nom du sujet dans le certificat; b) peut recevoir un autre nom dans le champ SubjectAlternativeName. Le DN doit se présenter sous la forme d'une chaîne imprimable X.501 et ne doit pas être vide.

3.1.2 Nécessité de l'utilisation de noms explicites

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Les champs de nom du sujet (Subject) et de l'émetteur (Issuer) doivent être liés au nom authentifié de l'entité. Dans le cas des personnes, le nom distinctif relatif (RDN) doit être une combinaison du prénom, du nom de famille et, facultativement, des initiales. Ce RDN peut aussi comprendre un poste ou un rôle organisationnel. Dans le cas des autres entités, le RDN correspondra au nom légal authentifié de l'entité. Lorsqu'un certificat correspond à un rôle ou à un poste, il doit aussi préciser l'identité de la personne qui occupe le poste ou qui assume le rôle en question.

3.1.3 Anonymat ou pseudo-anonymat des abonnés

L'identité du propriétaire d'un certificat n'est ni anonyme ni fictive. Lorsqu'un certificat est délivré à l'égard d'un rôle, l'identité du rôle et de la personne qui l'assument est indiquée.

Le masquage de l'identité du propriétaire d'un certificat pour des raisons de confidentialité est assuré par la politique de certification anonyme du GC.

3.1.4 Règles d'interprétation des diverses formes de noms

Les règles d'interprétation des formes de noms seront conformes au schéma de l'annuaire commun du GC, version 1.2 en date du 30 novembre 2000, tel que modifié ou révisé.

Le fait qu'un nom soit orthographié sans accent n'annule pas sa conformité au nom officiel.

3.1.5 Unicité des noms

Les noms distinctifs attribués à toutes les entités finales de l'AC doivent être uniques. Le champ SubjectUnique Identifiers, défini dans le profil de la LCR et du certificat d'infrastructure à clé publique Internet X.509, utilisé pour établir une distinction entre les abonnés ayant des noms identiques, ne sera pas supporté.

L'AC se réserve le droit de prendre des décisions au sujet des noms des entités dans tous les certificats attribués. On peut exiger d'une partie qui demande un certificat qu'elle démontre qu'elle a le droit d'utiliser un nom particulier.

En cas de litiges sur déclaration de nom dans un référentiel qui n'est pas sous son contrôle, l'AC doit s'assurer, dans son accord avec ce référentiel, que ce dernier a établi une procédure pour résoudre de tels litiges.

3.1.6 Reconnaissance, authentification et rôle des marques de commerce

Lorsque cela est permis ou requis, l'utilisation d'une marque de commerce est réservée au détenteur de cette marque.

3.2 Validation initiale de l'identité

3.2.1 Méthode de preuve de possession d'une clé privée

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Avant d'émettre un certificat de vérification, l'AC et l'entité finale doivent confirmer qu'elles sont en possession de la clé privée correspondante, d'une manière sûre.	Avant d'échanger une clé privée de déchiffrement, l'AC et l'entité finale doivent confirmer qu'elles sont en possession de la clé privée correspondante, d'une manière sûre.

3.2.2 Authentification de l'identité d'une organisation

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.

Les employés et les agents d'une organisation doivent présenter une demande pour être reconnus comme des abonnés, par l'intermédiaire d'une personne qui est habilitée à agir pour le compte de cette organisation.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance élevée	En plus d'être identifiée et authentifiée tel que décrit ci-après, la personne concernée doit se présenter à l'AC ou à l'AE, ou à un parrain du ministère qui l'a présentée personnellement à l'AC ou à l'AE, avant de se porter garant de cette personne, avant l'initialisation du jeton.

L'identité d'une organisation doit être authentifiée d'une manière satisfaisante pour l'AC, démontrant que l'organisation est bien celle qu'elle prétend être. L'authentification de l'identité de l'organisation peut être réalisée de l'une ou l'autre des manières suivantes :

a) Par le partage d'informations à titre privé, si l'identité de l'organisation a déjà été établie par un programme aux fins de l'instruction dans celui-ci;

b) Au moyen de copies de documents officiels prouvant l'existence de l'organisation.

L'AC ou l'AE doit également vérifier l'identité et l'autorité de la personne qui agit pour le compte de l'organisation, et s'assurer que cette personne est habilitée à recevoir les clés pour le compte de cette organisation.

L'AC ou l'AE doit s'assurer qu'une trace est conservée des moyens grâce auxquels l'identité de l'organisation et de la personne habilitée à agir pour le compte de cette dernière ont été établies, ainsi que de tout type de moyen d'identification utilisé, mais elle n'est pas tenue de conserver une copie des justificatifs d'identité eux-mêmes.

3.2.3 Authentification de l'identité d'une personne

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.

Personnes agissant pour leur propre compte

Un abonné potentiel peut présenter une demande pour son compte.

L'identité d'un abonné potentiel doit être authentifiée d'une manière satisfaisante qui permet à l'AC ou à l'AE d'établir que la personne est bien celle qu'elle affirme être. Avant que la demande soit présentée à l'AC, l'ALE doit authentifier l'identité de l'abonné potentiel, en se servant de l'un ou l'autre des moyens ci-après :

1. Par le partage d'informations à titre privé si l'identité de la personne a déjà été établie antérieurement;
2. Deux pièces d'identité (copies notariées ou originaux), dont l'une doit être une pièce d'identité émise par le gouvernement, avec photographie;
3. Des copies certifiées de deux pièces d'identité accompagnées de l'attestation d'une personne autorisée à agir comme répondant sur une demande de passeport canadien, attestation selon laquelle cette personne est bien celle qu'elle affirme être, selon le répondant;
4. Une signature numérique utilisant un certificat émis par une autre AC reconnue par l'AGP de l'ICP du GC, ou cocertifié avec le PIFC, pourvu que le niveau d'assurance du certificat de signature utilisé soit au moins égal au niveau d'assurance du certificat demandé.

Les ministères et organismes peuvent également exiger d'autres informations, preuves d'identité ou autorisations, pour permettre l'inscription à un programme.

L'AC ou l'AE doit s'assurer de conserver une trace des moyens grâce auxquels l'identité de la personne a été établie, ainsi que de tout type de document d'identité utilisé, mais elle n'est pas tenue de conserver une copie des documents d'identité eux-mêmes.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance élevée	En plus de satisfaire aux exigences d'identification et d'authentification, l'abonné potentiel doit se présenter personnellement à l'AC ou l'AE, ou à un parrain du ministère ou à une personne responsable désignée qui l'a présenté personnellement à l'AC ou à l'AE avant de se porter garant de cette personne, avant l'initialisation du jeton.

Personne agissant pour le compte d'une autre personne

Dans certaines circonstances exceptionnelles (par exemple un cas d'invalidité) autorisées par l'AC, une personne peut présenter une demande d'abonnement par l'entremise d'une autre personne autorisée à agir pour son compte.

Avant de présenter la demande à l'AC, l'ALE doit authentifier l'identité du demandeur et de l'abonné potentiel, en procédant de la même manière que pour une personne agissant pour son propre compte.

En outre, l'ALE doit également s'assurer que le demandeur est autorisé à agir pour le compte de l'abonné potentiel. La permission accordée par une personne à une autre, d'agir pour son compte, doit être attestée. Les circonstances qui nécessitent une telle permission doivent être autorisées par l'AC.

L'ALE doit fournir à l'AC les renseignements suivants :

1. L'Identification du demandeur et de l'abonné potentiel;
2. Une attestation selon laquelle l'identification et l'authentification ont été effectuées;
3. Une attestation selon laquelle le droit autorisant une personne à agir pour le compte d'une autre a été accordé, et que l'autorisation de l'AC a été obtenue;
4. Les coordonnées des personnes et de l'ALE permettant à l'AC ou à l'AE de communiquer avec elles.

L'AC ou l'AE doit s'assurer de conserver une trace des informations fournies par l'ALE à L'AC, ainsi que des moyens grâce auxquels l'identité a été établie et authentifiée, mais elle n'est pas tenue de conserver une copie des justificatifs d'identité.

L'AC ou l'AE doit s'assurer de conserver une trace des informations fournies par l'ALE à l'AC spécifiant les circonstances exceptionnelles, et authentifiant la permission pour une personne d'agir pour le compte d'une autre. Une trace de l'autorisation de l'AC doit être conservée.

Personnes qui représentent des rôles

Avant de présenter la demande à l'AC, l'ALE doit authentifier la personne qui demande la délivrance d'un certificat à l'égard d'un rôle à l'intérieur d'un ministère ou d'une organisation désignée, en procédant de la même façon que pour l'authentification d'un abonné individuel à l'intérieur d'un ministère ou d'une organisation désignée. L'ALE doit également s'assurer que cette personne est autorisée à assumer un tel rôle.

Lors de sa délivrance, le certificat sera délivré à la personne qui est autorisée à assumer le rôle et qui sera responsable de l'utilisation de ce certificat.

L'ALE doit fournir à l'AC les renseignements suivants :

1. Identification de la personne;
2. Attestation du fait que l'identification et l'authentification ont été effectuées;
3. Identification du rôle;
4. Coordonnées permettant à l'AC ou à l'AE de communiquer avec la personne et l'ALE.

L'AC ou l'AE doit conserver une trace du nom de la personne, de l'attestation effectuée par l'ALE et selon laquelle l'identification et l'authentification ont été effectuées, des moyens par lesquels l'identité du titulaire du rôle a été établie et authentifiée, ainsi que de tout type d'identification utilisé, mais elle n'est pas tenue de conserver une copie des justificatifs d'identité eux-mêmes.

Personnes agissant pour le compte d'un appareil ou d'une application

Avant de présenter la demande à l'AC, l'ALE doit authentifier la personne qui demande la délivrance d'un certificat à l'égard d'un appareil ou d'une application, en procédant de la même façon que pour un abonné individuel. L'ALE doit également s'assurer que cette personne est autorisée à être titulaire d'un certificat à l'égard d'un appareil ou d'une application.

Lors de la délivrance, le certificat sera délivré à la personne qui agit à titre de gardien et qui sera responsable de l'utilisation de ce certificat.

L'ALE doit fournir à l'AC les renseignements suivants :

1. Les informations d'identification de la personne;
2. Une attestation selon laquelle l'identification et l'authentification ont été effectuées;
3. L'identification de l'équipement (par exemple son numéro de série) ou de l'application (par exemple son nom DNS);
4. Les clés publiques de l'équipement ou de l'application;
5. L'autorisation et les attributs de l'équipement ou de l'application (s'ils doivent figurer sur le certificat);
6. L'approbation de l'AC attestant que l'application ou l'équipement satisfait aux exigences standard pour être jugé admissible à la délivrance d'un certificat (voir la section 3.2.6, Critères d'interopérabilité);
7. Les coordonnées du gardien et de l'ALE pour permettre à l'AC ou à l'AE de communiquer avec eux.

L'AC ou l'AE doit conserver une trace des informations fournies par l'ALE à l'AC, ainsi que des moyens grâce auxquels l'identité du gardien et de l'application ou de l'appareil a été établie et authentifiée, mais elle n'est pas tenue de conserver une copie des justificatifs d'identité eux-mêmes.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Lorsqu'un nom légal ou un nom d'organisation n'est pas utilisé à titre de RDN dans le certificat, l'AC doit conserver une trace du nom de la personne qui détient le certificat, lorsque celui-ci est délivré à l'égard d'un appareil, d'un rôle ou d'une application.

3.2.4 Renseignements non vérifiés sur l'abonné

Aucune exigence n'est stipulée.

3.2.5 Validation de l'autorité

On peut demander la délivrance d'un certificat à l'égard d'un appareil, d'une application ou d'un rôle. Les personnes qui sont identifiées à titre de gardien ou de titulaire du rôle correspondant au certificat délivré sont authentifiées pour s'assurer qu'elles possèdent bien l'autorité d'assumer cette fonction ou cette responsabilité, tel que stipulé dans la section 3.2.3.

À la discrétion de l'AC, un accord peut être établi, selon lequel une personne est autorisée à exercer le rôle de l'ALE dans son groupe spécifique :

- Une personne responsable désignée (PRD) est autorisée à agir à ce titre pour le compte d'une organisation à l'extérieur du GC qui désire enregistrer des abonnés pour des certificats émis par le GC;
- Un parrain ministériel est autorisé à agir à ce titre pour le compte d'un ministère.

Cet accord est établi uniquement lorsque le groupe concerné (organisation ou ministère) assume toutes les responsabilités à l'égard des activités d'identification et d'authentification accomplies, ainsi que de toutes les utilisations des certificats délivrés sous sa responsabilité.

L'identité d'un parrain ministériel ou d'une PRD potentielle doit être authentifiée de façon à permettre à l'AC de s'assurer que cette personne possède bien l'identité qu'elle affirme posséder. L'AC, en consultation avec les responsables concernés du ministère ou de l'organisation ou les propriétaires responsables de l'application, doivent également confirmer que le candidat est autorisé par le ministère ou l'organisation à agir pour son compte à ce titre.

L'AC ou l'AE doit authentifier l'identité du candidat à la fonction d'ALE, par l'un quelconque des moyens suivants :

1. Information partagée à titre privé si l'identité de la personne a déjà été antérieurement établie;
2. Deux pièces d'identité (copies notariées ou originaux), dont l'une doit être une pièce d'identité émise par le gouvernement, avec photographie;
3. Des copies certifiées de deux pièces d'identité accompagnées de l'attestation d'une personne autorisée à agir comme répondant sur une demande de passeport canadien, attestation selon laquelle cette personne est bien celle qu'elle prétend être, selon le répondant;
4. Une signature numérique utilisant un certificat délivré par une autre AC reconnue par l'AGP de l'ICP du GC ou cocertifié avec le PIFC, pourvu que le niveau d'assurance du certificat de signature utilisé soit au moins égal au niveau d'assurance du certificat demandé.

L'AC ou l'AE doit conserver une trace des moyens grâce auxquels l'identité de l'ALE a été établie et authentifiée, ainsi que de tout type d'identification utilisé, mais elle n'est pas tenue de conserver une copie des justificatifs d'identité eux-mêmes.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance élevée	En plus d'être identifié et authentifié, le parrain ministériel ou la PRD doit se présenter personnellement à l'AC ou à l'AE, avant de pouvoir se porter garant de l'identité d'un abonné potentiel à l'égard duquel on a demandé la délivrance de certificats de niveau d'assurance élevée.

3.2.6 Critères d'interopérabilité

En ce qui concerne les accords de certification croisée et la reconnaissance des autres AC, l'AC est régie par la « politique de gestion de l'ICP du GC ». L'AC, pour présenter une demande de certification croisée, doit impérativement passer par le pont de l'ICP fédérale canadienne (PIFC). Les critères et la marche à suivre détaillés sont décrits dans la méthode d'assurance de la confiance de l'AC du GC.

3.3 Identification et authentification des demandes de renouvellement de clé

3.3.1 Identification et authentification des demandes de renouvellement de clé courantes

Une demande de renouvellement de clé peut être présentée par l'entité au nom de laquelle les clés ont été émises, ou par une autre personne autorisée à agir pour le compte de l'entité, tel qu'indiqué dans la section 3.2.3. Toutes les demandes de renouvellement de clé doivent être authentifiées par l'AC, et la réponse subséquente doit être authentifiée par l'entité ou par une autre personne autorisée à agir pour le compte de cette dernière.

Une entité qui demande le renouvellement d'une clé peut authentifier la demande au moyen de sa paire de clés de signature numérique valide.

Quand une des clés est arrivée à expiration, la demande de renouvellement doit être authentifiée comme s'il s'agissait d'un enregistrement initial.

Les demandes de renouvellement courantes des clés doivent être enregistrées dans un journal.

3.3.2 Identification et authentification d'une demande de renouvellement de clé après la révocation de cette dernière

Lorsque l'information contenue dans un certificat a changé ou qu'il existe une compromission réelle ou présumée d'une clé privée, l'AC doit authentifier la demande de renouvellement de la clé comme s'il s'agissait d'un enregistrement initial.

Tout changement apporté à l'information contenue dans un certificat doit être vérifié par l'AC ou une AE autorisée à agir pour le compte de cette AC, avant que le certificat soit délivré, sauf lorsque l'AC a déterminé que les changements multiples apportés aux DN des abonnés résultaient de changements organisationnels dans un ministère ou une organisation désignée.

Les demandes de renouvellement de clé après la révocation doivent être enregistrées dans un journal.

3.4 Identification et authentification des demandes de révocation

La section 4.9.2 indique qui peut demander la révocation d'un certificat.

L'AC ou l'AE doit authentifier la demande de révocation du certificat. L'authentification peut être effectuée au moyen d'informations partagées à titre privé.

Une entité qui demande la révocation peut authentifier sa demande au moyen de sa clé de signature privée, peu importe que cette clé de signature privée ait été compromise ou non.

L'AC doit établir et rendre publique la procédure de traitement de ces demandes, ainsi que les moyens qu'elle utilise pour établir leur validité.

Les demandes de révocation de certificat doivent être enregistrées dans un journal.

4. EXIGENCES OPÉRATIONNELLES DU CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Qui peut présenter une demande de certificat

Les types de demandeurs autorisés à titre d'abonnés du GC sont indiqués dans la section 1.3.3.

Les demandes de certificats en lots (ou en masse) sont permises, mais elles peuvent être présentées uniquement par des personnes autorisées à faire de telles demandes.

4.1.2 Processus d'inscription et responsabilités

Les personnes qui désirent obtenir un certificat doivent être autorisées et approuvées par une AE ou une ALE. Les responsabilités de l'AE ou de l'ALE dans le traitement des divers types de demandes sont décrites dans la section 1.3 (Participants à l'ICP) et la section 3.2 (Validation de l'identité).

La demande de certificat est distincte de tout processus du ministère ou de l'organisme pour s'inscrire dans un programme ou utiliser ce dernier. Le PRA peut imposer des exigences additionnelles et demander, pour accorder l'accès à un programme, des renseignements, des justificatifs ou des autorisations additionnels.

4.2 Traitement des demandes de certificats

L'AC doit :

1. décrire dans l'EPC toutes les procédures et les exigences concernant les demandes de délivrance d'un certificat;
2. indiquer aux abonnés potentiels les renseignements qu'ils doivent présenter ainsi que la marche à suivre pour la demande.

4.2.1 Fonctions d'identification et d'authentification

L'AC doit s'assurer que chaque demande est accompagnée de ce qui suit :

1. Une preuve ou une confirmation de l'identité de l'entité finale, conformément aux sections 3.2.2 et 3.2.3;
2. Sur demande de l'AC, une preuve ou une confirmation de l'autorisation du certificat demandé;
3. Sur demande de l'AC, une preuve ou une confirmation de l'autorisation des attributs du certificat demandé.

En outre, dans le cas des demandes approuvées, l'ALE doit indiquer qu'il existe un accord avec l'AC pour l'enregistrement, en ce qui concerne l'organisation locale spécifique concernée :

- Les PRD doivent indiquer le nom de l'organisation désignée, la date d'exécution de l'accord ou l'identificateur de contrat pour indiquer l'accord que leur organisation a signé concernant ses droits, ses privilèges et ses obligations associées aux certificats délivrés, ou qui seront délivrés, pour le compte de l'organisation désignée;
- Les parrains ministériels doivent référencer les politiques du ministère qui indiquent que ce dernier a établi les droits, les privilèges et les obligations des employés du ministère associés aux certificats délivrés, ou qui seront délivrés, à ces employés pour qu'ils s'en servent pour le compte du ministère.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE
Assurance rudimentaire	Chaque demande peut être accompagnée par une clé de vérification publique générée par l'abonné ou pour son compte.
Assurance de base **Assurance moyenne** **Assurance élevée**	Chaque application doit être accompagnée par une clé de vérification publique générée par l'abonné ou pour son compte.

4.2.2 Approbation ou rejet des demandes de certificats

L'AC délivre le certificat uniquement une fois que la demande de certificat a été approuvée de façon complète et définitive.

La présentation d'une demande de certificat n'oblige pas l'AC à émettre ce certificat. À sa seule discrétion, l'AC peut refuser d'émettre un certificat à l'égard d'une demande reçue.

4.2.3 Délai de traitement des demandes de certificats

NIVEAU D'ASSURANCE	EXIGENCES
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base	Aucune exigence n'est stipulée concernant la période écoulée entre la réception de la demande de certificat et la génération de la clé de l'entité. L'AC doit s'assurer que la période dont l'entité dispose pour accomplir le processus d'initialisation ne dépasse pas 30 jours ouvrables.
Assurance moyenne	Aucune exigence n'est stipulée concernant la période écoulée entre la réception de la demande de certificat et la génération de la clé de l'entité. L'AC doit s'assurer que la période dont l'entité dispose pour accomplir le processus d'initialisation ne dépasse pas 21 jours ouvrables.
Assurance élevée	Aucune exigence n'est stipulée concernant la période écoulée entre la réception de la demande de certificat et la génération de la clé de l'entité. L'AC doit s'assurer que l'entité accomplit le processus d'initialisation immédiatement sur réception des données d'activation.

4.3 Émission des certificats

La délivrance ou l'émission d'un certificat par l'AC indique que cette dernière a approuvé complètement et de façon définitive la demande de certificat.

Le processus de délivrance d'un certificat par l'AC est distinct de tout processus du ministère ou de l'organisme visant l'inscription dans un programme ou l'utilisation de celui-ci.

4.3.1 Actions de l'AC lors de la délivrance des certificats

Aucune exigence n'est stipulée.

4.3.2 Notification à l'abonné par l'AC de la délivrance du certificat

Sauf mention expresse du contraire, la publication d'un certificat dans un référentiel constitue la certification de l'AC, et un avis à un abonné ou à une partie utilisatrice qui peut accéder au certificat dans le référentiel, que les renseignements qui figurent dans ce certificat ont été vérifiés conformément aux présentes politiques de certification.

4.4 Acceptation du certificat

4.4.1 Conduite constituant l'acceptation du certificat

L'utilisation du certificat par un abonné ou un rôle, un appareil ou une application à l'égard duquel un certificat a été émis constitue l'acceptation de ce certificat et de toutes les obligations associées à son utilisation.

4.4.2 Publication du certificat par l'AC

Sauf mention expresse du contraire, la publication d'un certificat dans un référentiel constitue la certification de l'AC, et un avis à un abonné ou à une partie utilisatrice qui peut accéder au certificat dans le référentiel, que les renseignements qui figurent dans ce certificat ont été vérifiés conformément aux présentes politiques de certification.

4.4.3 Notification de la délivrance d'un certificat par l'AC aux autres entités

Aucune exigence n'est stipulée.

4.5 Utilisation des paires de clés et des certificats

4.5.1 Utilisation de la clé privée et du certificat de l'abonné

L'AC doit s'assurer que les certificats qu'elle émet sont soumis à des termes et conditions d'utilisation. Les abonnés sont alors assujettis à ces termes et conditions, que ces derniers figurent dans un accord ou un autre document, et qui concernent leurs droits, privilèges et obligations associés aux certificats qui leur sont délivrés.

Avant que l'AC délivre un certificat à une personne en vue d'une utilisation dans le cadre d'un programme, ce programme doit être certifié. Le PRA doit certifier l'application, conformément aux critères d'interopérabilité de la section 3.2.6.

4.5.2 Utilisation du certificat et de la clé publique par une partie utilisatrice

Une partie utilisatrice doit effectuer les opérations cryptographiques prévues au moyen des certificats reconnus par l'AC, tel que stipulé dans la section 3.2.6.

Les déclarations et les garanties de la partie utilisatrice sont stipulées dans la section 9.6.4.

4.6 Renouvellement d'un certificat

4.6.1 Circonstances du renouvellement d'un certificat

Aucune exigence n'est stipulée.

4.6.2 Qui peut demander le renouvellement

Aucune exigence n'est stipulée.

4.6.3 Traitement des demandes de renouvellement de certificats

Aucune exigence n'est stipulée.

4.6.4 Notification de la délivrance d'un nouveau certificat à l'abonné

Aucune exigence n'est stipulée.

4.6.5 Conduite constituant l'acceptation d'un certificat renouvelé

Aucune exigence n'est stipulée.

4.6.6 Publication par l'AC du certificat renouvelé

Aucune exigence n'est stipulée.

4.6.7 Notification de la délivrance d'un certificat par l'AC aux autres entités

Aucune exigence n'est stipulée.

4.7 Renouvellement d'un certificat

4.7.1 Circonstances du renouvellement d'un certificat

Un certificat peut être renouvelé pour l'une ou l'autre des raisons suivantes :

1) La durée de vie de la clé et du certificat arrivent à échéance;
2) Le certificat a été révoqué et un nouveau certificat est autorisé (l'abonné demeure toujours un abonné valide).

Un certificat ne doit pas être admissible à un renouvellement automatique lorsqu'il a été révoqué ou suspendu.

4.7.2 Qui peut demander la certification d'une nouvelle clé publique

Une demande de renouvellement de clés peut être présentée par l'entité au nom de laquelle les clés ont été émises, ou par une autre personne autorisée à agir pour le compte de cette entité. Toutes les demandes de renouvellement de clés doivent être authentifiées par l'AC, et la réponse subséquente doit être authentifiée par l'entité ou par une autre personne autorisée à agir pour le compte de l'entité.

4.7.3 Traitement des demandes de renouvellement de certificats

Lorsqu'une des clés est arrivée à échéance, la demande de renouvellement de clés doit être authentifiée de la même manière que pour l'enregistrement initial.

Une entité qui demande le renouvellement d'une clé peut authentifier la demande au moyen de sa paire de clés de signature numérique valide.

Les demandes de renouvellement de clés courantes doivent être enregistrées dans un journal.

4.7.4 Notification de la délivrance d'un nouveau certificat à l'abonné

Conformément à la section 4.3.2 (Notification à l'abonné par l'AC de la délivrance d'un certificat).

4.7.5 Conduite constituant l'acceptation d'un certificat renouvelé

Conformément à la section 4.4.1 (Conduite constituant l'acceptation d'un certificat).

4.7.6 Publication du certificat renouvelé par l'AC

Conformément à la section 4.4.2 (Publication du certificat par l'AC).

4.7.7 Notification de la délivrance du certificat par l'AC à d'autres entités

Conformément à la section 4.4.3 (Notification de la délivrance du certificat par l'AC aux autres entités).

4.8 Modification d'un certificat

4.8.1 Circonstances de modification d'un certificat

Aucune exigence n'est stipulée.

4.8.2 Qui peut demander la modification d'un certificat

Aucune exigence n'est stipulée.

4.8.3 Traitement des demandes de modification d'un certificat

Aucune exigence n'est stipulée.

4.8.4 Notification de la délivrance d'un nouveau certificat à l'abonné

Aucune exigence n'est stipulée.

4.8.5 Conduite constituant l'acceptation d'un certificat modifié

Aucune exigence n'est stipulée.

4.8.6 Publication du certificat modifié par l'AC

Aucune exigence n'est stipulée.

4.8.7 Notification de la délivrance d'un certificat par l'AC aux autres entités

Aucune exigence n'est stipulée.

4.9 Révocation ou suspension d'un certificat

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
En cas de compromission présumée de la clé de signature de l'AC, celle-ci doit immédiatement aviser toutes les AC auxquelles elle a émis des certificats croisés ainsi que l'AGP de l'ICP du GC. En cas de compromission de la clé de signature de l'AC, celle-ci doit respecter les obligations décrites dans la section 5.7.1. En cas de compromission réelle ou présumée de la clé de signature de toute autre entité, celle-ci doit aviser l'AC sur-le-champ.	En cas de compromission réelle ou présumée de la clé privée de déchiffrement d'une entité, celle-ci doit aviser l'AC sur-le-champ.

Le cas de la compromission de l'AC est décrit dans la section 5.7.1, Traitement des incidents.

4.9.1 Motifs de révocation

Sur réception d'un avis acceptable, l'AC doit révoquer un certificat pour les motifs suivants :

1. Quand une information quelconque dans le certificat change;
2. En cas de compromission réelle ou présumée de la clé privée ou du support sur lequel elle est enregistrée;
3. En cas de décès ou de cessation d'emploi de l'abonné;
4. En cas de cessation des activités d'un appareil, d'une application ou d'un rôle;
5. Lorsqu'un abonné ou un détenteur de certificat présente une demande adéquatement authentifiée afin de révoquer son certificat.

L'AC peut révoquer, à sa discrétion, un certificat lorsqu'une entité omet de se conformer à toute entente ou toute loi applicable, lorsque l'abonné ou le détenteur du certificat n'a pas utilisé ses clés privées depuis plus de 18 mois, ou lorsque l'AC a des motifs raisonnables de croire que cela est approprié, compte tenu des circonstances.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE et CONFIDENTIALITÉ
Assurance rudimentaire	L'AC peut avertir une entité que le certificat qui lui avait été attribué a été révoqué.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit avertir une entité lorsqu'elle révoque un certificat qui lui a été attribué.

4.9.2 Qui peut demander la révocation

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée concernant les certificats des entités finales.
Assurance de base **Assurance moyenne** **Assurance élevée**	La révocation d'un certificat peut être demandée uniquement par : 1. Un abonné; 2. Une personne autorisée à agir pour le compte de l'abonné, tel que spécifié dans la section 3.2.3; 3. Une ALE à laquelle on a confié la responsabilité d'administrer les demandes de révocation des certificats des abonnés; 4. Le gardien d'un certificat délivré à l'égard d'un rôle, d'un appareil ou d'une application; 5. Le personnel autorisé de l'AC, à sa propre discrétion ou sur demande d'un abonné, de l'ALE ou du gardien; 6. Un processus automatisé agissant pour le compte de l'AC; 7. Un programme du GC.

La révocation d'un certificat croisé (cocertificat) peut être demandée uniquement par :

1. L'AC à laquelle le cocertificat a été émis;
2. Le personnel autorisé du PIFC;
3. L'AGP de l'ICP du GC.

Le cas de la compromission de l'AC est décrit dans la section 5.7.1, Traitement des incidents.

4.9.3 Procédure de demande de révocation

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit : 1. authentifier l'identité et l'autorité de toutes les demandes de révocation conformément à la section 3.4; 2. consigner et conserver toutes les informations concernant de telles demandes, y compris un énoncé décrivant les actions entreprises par l'AC; 3. publier l'avis de révocation du certificat dans son serveur LCR ou OCSP; 4. publier l'avis de révocation du certificat croisé dans son serveur LAR ou OCSP.

4.9.4 Période de grâce des demandes de révocation

L'abonné doit immédiatement avertir l'AC, de la manière spécifiée par l'AC, en cas de compromission réelle ou présumée des clés privées, du mot de passe ou des jetons de clé de l'abonné.

4.9.5 Délai à l'intérieur duquel l'AC doit traiter la demande de révocation

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base	Toute mesure prise à la suite de la demande de révocation d'un certificat doit l'être : 1. immédiatement, si la demande est reçue pendant les heures normales d'ouverture de l'AC; 2. immédiatement au début du jour ouvrable suivant, si la demande est reçue en dehors des heures normales d'ouverture; 3. au plus tard vingt-quatre (24) heures après la réception de la demande, si celle-ci est reçue en dehors des heures normales d'ouverture et si le jour suivant n'est pas un jour ouvrable.
Assurance moyenne	Toute mesure prise à la suite de la demande de révocation d'un certificat doit l'être : 1. immédiatement, si la demande est reçue pendant les heures normales d'ouverture de l'AC; 2. immédiatement au début du jour ouvrable suivant, si la demande est reçue en dehors des heures normales d'ouverture; 3. au plus tard douze (12) heures après la réception de la demande, si celle-ci est reçue en dehors des heures normales d'ouverture et si le jour suivant n'est pas un jour ouvrable.
Assurance élevée	Toute mesure prise à la suite d'une demande de révocation d'un certificat doit l'être immédiatement sur réception de la demande.

4.9.6 Exigences concernant la révocation applicables aux parties utilisatrices

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne**	La partie utilisatrice doit : a. vérifier l'état de tous les certificats dans la chaîne de validation des certificats, en fonction des LCR et des LAR à jour, avant d'utiliser ces certificats; b. vérifier l'authenticité et l'intégrité des LCR et des LAR.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance élevée	La partie utilisatrice doit : a. vérifier l'état de tous les certificats dans la chaîne de validation des certificats, en fonction des LCR et des LAR à jour, avant d'utiliser ces certificats; b. vérifier l'authenticité et l'intégrité des LCR et des LAR. En outre, les entités finales de niveau d'assurance élevée ne doivent pas cacher les informations concernant les certificats révoqués.

4.9.7 Fréquence de publication de la LCR

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base	L'AC doit publier une LCR à jour au moins aux vingt-quatre (24) heures. L'AC doit également s'assurer que la publication de cette LCR est synchronisée avec tous les référentiels pertinents, afin de permettre à la partie utilisatrice de consulter la LCR la plus récente. Dans le cas de la compromission réelle ou présumée d'une clé, l'AC doit publier une LCR à jour immédiatement sur révocation du certificat.
Assurance moyenne	L'AC doit publier une LCR à jour au moins aux douze (12) heures. L'AC doit également s'assurer que la publication de cette LCR est synchronisée avec tous les référentiels pertinents, afin de permettre à la partie utilisatrice de consulter la LCR la plus récente. Dans le cas de la compromission réelle ou présumée d'une clé, l'AC doit publier une LCR à jour immédiatement sur révocation du certificat.
Assurance élevée	L'AC doit publier une LCR à jour au moins aux quatre (4) heures. L'AC doit également s'assurer que la publication de cette LCR est synchronisée avec tous les référentiels pertinents, afin de permettre à la partie utilisatrice de consulter la LCR la plus récente. Dans le cas de la compromission réelle ou présumée d'une clé, l'AC doit publier une LCR à jour immédiatement sur révocation du certificat.

4.9.8 Temps de latence maximum des LCR (le cas échéant)

Aucune exigence n'est stipulée.

4.9.9 Disponibilité de la vérification en ligne de l'état et de la révocation

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base	Lorsque des serveurs OCSP sont utilisés à l'appui d'un programme, l'AC doit diffuser les avis de révocation sur ces serveurs au moins aux vingt-quatre (24) heures.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
	Dans le cas de la compromission réelle ou présumée d'une clé, l'AC doit publier une LCR à jour immédiatement sur révocation du certificat.
Assurance moyenne	Lorsque des serveurs OCSP sont utilisés à l'appui d'un programme, l'AC doit diffuser les avis de révocation sur ces serveurs au moins aux douze (12) heures. Dans le cas de la compromission réelle ou présumée d'une clé, l'AC doit publier une LCR à jour immédiatement sur révocation du certificat.
Assurance élevée	Lorsque des serveurs OCSP sont utilisés à l'appui d'un programme, l'AC doit diffuser les avis de révocation sur ces serveurs au moins aux quatre (4) heures. Dans le cas de la compromission réelle ou présumée d'une clé, l'AC doit publier une LCR à jour immédiatement sur révocation du certificat.

4.9.10 Exigences relatives à la vérification en ligne de la révocation

Lorsque des serveurs OCSP sont utilisés, une partie utilisatrice doit vérifier l'état de tous les certificats pertinents dans le serveur OCSP avant d'utiliser ces certificats.

4.9.11 Autres formes de publication des certificats révoqués

Aucune exigence n'est stipulée.

4.9.12 Exigences spéciales concernant la compromission des clés

Ces exigences sont stipulées dans les sections 4.9.7 (Fréquence de publication de la LCR) et 4.9.9 (Disponibilité de la vérification en ligne de la révocation et de l'état).

4.9.13 Circonstances de la suspension

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base	L'AC peut effectuer l'équivalent d'une suspension en révoquant le certificat avec le motif « en suspens ». Cette révocation temporaire d'un certificat ne modifie pas les obligations de l'abonné à l'égard de la clé privée associée à ce certificat.
Assurance moyenne	L'AC peut temporairement révoquer un certificat, lorsqu'il y a compromission présumée de la clé privée ou du support sur lequel la clé privée est enregistrée.
Assurance élevée	L'AC peut, à sa discrétion, révoquer temporairement un certificat lorsqu'une entité omet de se conformer à toute entente ou toute loi applicable, après un nombre prédéterminé de tentatives infructueuses d'ouverture de session par un abonné, ou lorsque l'AC a des motifs raisonnables de croire que cela est approprié, compte tenu des circonstances.

4.9.14 Qui peut demander la suspension

Tel que stipulé dans la section 4.9.2 (Qui peut demander la révocation).

4.9.15 Procédure de demande de suspension

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit : 1. authentifier toutes les demandes de révocation temporaire d'un certificat; 2. enregistrer et conserver tous les renseignements concernant ces demandes, notamment une déclaration au sujet des mesures prises par l'AC; 3. publier un avis de révocation temporaire du certificat dans son serveur de LCR ou OCSP.

4.9.16 Limites de la période de suspension

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC peut mettre fin à la révocation temporaire d'un certificat lorsqu'elle détermine que les raisons de la révocation temporaire n'étaient pas fondées ou que le certificat doit être révoqué pour un motif autre que « en suspens ».

4.10 Services d'état des certificats

L'AC est responsable de promulguer l'état des certificats dans les LCR et les LAR.

4.10.1 Caractéristiques opérationnelles

Les caractéristiques des LCR sont stipulées dans la section 7.2 (Profil des LCR).

Les caractéristiques OCSP sont stipulées dans la section 7.3 (Profil OCSP).

4.10.2 Disponibilité du service

Les exigences concernant la disponibilité du service de LCR sont stipulées dans la section 4.9.7 (Fréquence de publication de la LCR).

Les exigences concernant la disponibilité du service OCSP sont stipulées dans la section 4.9.9 (Disponibilité de la vérification en ligne de la révocation et de l'état).

4.10.3 Caractéristiques optionnelles

Aucune exigence n'est stipulée.

4.11 Fin de l'abonnement

Les exigences correspondantes sont stipulées dans la section 4.9.1 (Circonstances de la révocation).

4.12 Séquestre et récupération des clés

4.12.1 Politique et pratiques de séquestre et de récupération des clés

L'AC ne doit pas participer au séquestre des clés privées par un tiers.

4.12.2 Politique et pratiques d'encapsulation et de récupération des clés de session

Aucune exigence n'est stipulée.

4.13 Historique et récupération des clés

L'AC doit saisir l'historique des clés de déchiffrement de l'abonné à la suite du renouvellement du certificat, conformément à la section 4.7. Le stockage des clés par l'AC doit être utilisé strictement à des fins de récupération des clés et de continuité des activités.

5. INSTALLATIONS, GESTION ET CONTRÔLES OPÉRATIONNELS

5.1 Contrôles physiques

5.1.1 Emplacement et construction des installations

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	L'AC doit s'assurer que les installations informatiques qui hébergent les services de l'AC, y compris les autorités d'enregistrement automatisé : 1. satisfont au minimum aux exigences applicables à une **zone de travail**; 2. sont surveillées manuellement ou électroniquement, afin d'empêcher les intrusions non autorisées en tout temps. Lorsque des postes de travail d'AE non automatisés sont utilisés, chaque poste de travail d'AE doit être situé dans des locaux satisfaisant aux critères d'une **zone d'accueil**.
Assurance de base	L'AC doit s'assurer que les informations informatiques qui hébergent les services de l'AC, y compris les autorités d'enregistrement automatisé : 1. satisfont au minimum aux exigences applicables à une **zone de sécurité**; 2. sont surveillées manuellement ou électroniquement, afin d'empêcher les intrusions non autorisées en tout temps. Si des postes de travail d'AE non automatisés sont utilisés, chaque poste de travail d'AE doit être situé dans des locaux satisfaisant aux critères d'une **zone d'accueil**. Lorsqu'une AE non automatisée est autorisée à présenter des demandes en ligne dans une session avec l'AC, l'AC doit s'assurer que l'exploitation du site de l'AE offre une protection suffisante pour le module cryptographique et la clé privée de l'administrateur de l'AE. L'AC doit s'assurer qu'une évaluation des menaces et des risques est effectuée concernant le module cryptographique de l'AE. Par exemple, le module cryptographique et la clé privée de l'administrateur de l'AE peuvent être conservés dans un coffre ou un contenant de sécurité.
Assurance moyenne	L'AC doit s'assurer que les installations informatiques qui hébergent les services de l'AE, y compris les autorités d'enregistrement automatisé : 1. satisfont au minimum aux exigences applicables à une **zone de sécurité**; 2. sont surveillées manuellement ou électroniquement, afin d'empêcher les intrusions non autorisées en tout temps. Lorsque des postes de travail d'AE non automatisés sont utilisés, chaque poste de travail d'AE doit être situé dans : 1. une **zone de travail**; ou 2. une **zone d'accueil** lorsque les postes sont occupés, la sécurité de tous les supports étant assurée lorsque les postes ne sont pas occupés. Lorsqu'une AE non automatisée est autorisée à présenter des demandes en ligne dans une session avec l'AC, l'AC doit s'assurer que l'exploitation du site de l'AE offre une protection suffisante au module cryptographique et à la clé privée de l'administrateur de l'AE. L'AC doit s'assurer qu'une évaluation des

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
	menaces et des risques est effectuée concernant le module cryptographique de l'AE. Par exemple, le module cryptographique et la clé privée de l'administrateur de l'AE peuvent être conservés dans un coffre ou un contenant de sécurité.
Assurance élevée	L'AC doit s'assurer que les installations informatiques qui hébergent les services de l'AC, y compris les autorités d'enregistrement automatisé : 1. satisfont au minimum aux exigences applicables à une **zone de sécurité**; 2. sont surveillées manuellement ou électroniquement, afin d'empêcher les intrusions non autorisées en tout temps. Lorsque des postes de travail d'AE non automatisés sont utilisés, chaque poste de travail d'AE doit être situé dans une **zone de sécurité**, ou une zone de travail lorsque les postes sont occupés, tous les supports étant protégés lorsque les postes ne sont pas occupés. **En plus de satisfaire aux exigences applicables à une AC, le PIFC doit satisfaire aux exigences applicables à une zone de haute sécurité.** Lorsqu'une AE non automatisée est autorisée à présenter des demandes en ligne dans une session avec l'AC, l'AC doit s'assurer que l'exploitation du site de l'AE offre un degré de sécurité suffisant pour le module cryptographique et la clé privée de l'administrateur de l'AE. L'AC doit s'assurer qu'une évaluation des menaces et des risques est effectuée concernant le module cryptographique de l'AE. Par exemple, le module cryptographique et la clé privée de l'administrateur de l'AE peuvent être conservés dans un coffre ou un contenant de sécurité.

5.1.2 Accès physique

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Lorsqu'un NIP ou un mot de passe est enregistré pour un site d'une AC ou d'une AE, il doit être conservé dans un contenant de sécurité accessible uniquement au personnel autorisé.
Assurance de base **Assurance moyenne**	En ce qui concerne l'emplacement du matériel et du logiciel de l'AC, l'AC doit s'assurer que : 1. l'accès sans escorte au serveur de l'AC est limité aux personnels dont le nom figure sur la liste de contrôle d'accès; 2. le personnel dont le nom ne figure pas sur la liste de contrôle d'accès est accompagné et supervisé de manière adéquate; 3. un journal des accès au site est tenu à jour et inspecté chaque semaine. L'AC doit s'assurer que tous les supports amovibles et tous les documents papier qui contiennent de l'information sensible en clair sont conservés dans des contenants qui figurent dans le Guide de l'équipement de sécurité du GC ou d'une résistance équivalente. Lorsqu'un NIP ou un mot de passe est enregistré pour un site d'une AC ou d'une AE, il doit être conservé dans un contenant de sécurité accessible uniquement au personnel autorisé. Les abonnés ne doivent pas laisser leur poste de travail sans surveillance lorsque les protections cryptographiques sont débloquées (c'est-à-dire

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
	lorsque le NIP ou le mot de passe a été entré). Un poste de travail qui contient des clés privées dans son disque dur doit être protégé physiquement ou au moyen d'un produit de contrôle d'accès approprié.
Assurance élevée	En ce qui concerne l'emplacement du matériel et du logiciel de l'AC, l'AC doit s'assurer que : 1. l'accès sans escorte au serveur de l'AC est limité aux seuls personnels dont le nom figure sur une liste de contrôle d'accès; 2. le personnel dont le nom ne figure pas sur la liste de contrôle d'accès est accompagné et supervisé de manière adéquate; 3. un journal des accès au site est tenu à jour et inspecté chaque semaine. L'AC doit s'assurer que tous les supports amovibles et les documents papier qui contiennent de l'information sensible en clair sont conservés dans des contenants qui figurent dans le Guide de l'équipement de sécurité du GC ou d'une résistance équivalente. Lorsqu'un NIP ou un mot de passe est enregistré pour un site d'AC ou d'AE, il doit être conservé dans un contenant de sécurité accessible uniquement au personnel autorisé. Les abonnés ne doivent pas laisser leur poste de travail sans surveillance lorsque la protection cryptographique est débloquée (c'est-à-dire lorsque le NIP ou le mot de passe a été entré). Un poste de travail qui contient des clés privées sur un disque dur doit être protégé physiquement ou au moyen d'un produit de contrôle d'accès approprié. Le module cryptographique matériel de l'abonné doit être protégé physiquement. Cette protection peut être assurée au moyen de la protection du site ou par l'abonné qui conserve alors le module cryptographique matériel avec lui.

5.1.3 Alimentation électrique et climatisation

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit s'assurer que les installations d'alimentation électrique et de climatisation sont suffisantes pour permettre le bon fonctionnement du système de l'AC.

5.1.4 Exposition à l'eau

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit s'assurer que le système de l'AC est adéquatement protégé contre l'exposition à l'eau.

5.1.5 Prévention et protection contre les incendies

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit s'assurer que le système de l'AC est adéquatement protégé contre les incendies grâce à un système d'extinction des incendies.

5.1.6 Stockage des supports

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit s'assurer que les supports de stockage utilisés par le système de l'AC sont protégés contre les menaces environnementales comme la température, l'humidité et le magnétisme.

5.1.7 Élimination des déchets

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit s'assurer que tous les supports qui contiennent de l'information sensible sont nettoyés, afin d'enlever toute information, de sorte qu'il soit impossible de récupérer les données, ou encore que ces supports soient détruits avant leur radiation. Le personnel de l'AC doit consigner la destruction de l'information sensible.

5.1.8 Sauvegarde hors site

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit s'assurer qu'elle utilise des installations situées dans un lieu séparé de celui de l'AC, aux fins de la sauvegarde et de l'archivage hors site. L'AC doit s'assurer que : 1. les installations servant à la sauvegarde et à l'archivage hors site : a) ont le même niveau de sécurité que le site primaire de l'AC; b) sont correctement protégées contre les menaces environnementales comme la température, l'humidité et le magnétisme; 2. la transmission et/ou le transport du matériel à sauvegarder et à archiver, en provenance de l'AC vers les installations de sauvegarde hors site, doit se faire d'une manière sûre.

5.2 Contrôles procéduraux

5.2.1 Rôles de confiance

Rôles de confiance de l'AC

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Une AC peut permettre que toutes les tâches associées aux fonctions critiques de l'AC soient effectuées par une même personne.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit assurer la séparation des tâches à l'égard des fonctions critiques de l'AC, pour empêcher qu'une seule personne puisse utiliser de façon malveillante le système de l'AC sans que cela soit détecté. L'accès au système de chaque utilisateur doit être limité aux seules actions requises par cette personne dans l'exécution de ses tâches. L'AC doit prévoir au moins trois (3) rôles distincts pour le personnel de l'ICP, afin d'établir une distinction entre l'exploitation au jour le jour du système de l'AC; la gestion de ces opérations; et la gestion des changements substantiels qui sont apportés aux exigences du système, notamment aux politiques, aux procédures ou au personnel. Ces rôles doivent être assumés par le personnel désigné comme suit : a) utilisateur maître de l'ICP;

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
	b) responsable de la sécurité de l'ICP; c) administrateur de l'ICP; et ceux-ci doivent avoir au minimum les responsabilités décrites dans la section 1.3.1. Toute autre séparation des responsabilités est permise, pourvu qu'elle offre le même degré de résistance aux « attaques de l'intérieur ». Seuls l'utilisateur maître de l'ICP et le personnel responsable de l'installation du matériel et du système d'exploitation, ou le personnel accompagné par eux, doivent pouvoir accéder physiquement aux logiciels qui contrôlent le système de l'AC. Le personnel de l'AC ne doit pas auditer ses propres activités.

Rôles de confiance de l'AE

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Une AC doit s'assurer que le personnel de l'AE comprend ses responsabilités à l'égard de l'identification et de l'authentification des abonnés potentiels. Le personnel de l'AE doit avoir, au moins, les responsabilités établies dans la section 1.3.2. Une AC peut permettre que toutes les tâches correspondant aux fonctions de l'AE soient accomplies par une seule personne.

5.2.2 Nombre de personnes requises par tâche

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit s'assurer qu'aucune personne ne puisse accéder aux clés privées des abonnés stockées par l'AC. Au moins deux personnes doivent être nécessaires pour accomplir les tâches sensibles, ces dernières étant définies dans l'EPC. L'AC peut permettre aux abonnés d'effectuer de manière sûre leurs propres opérations de récupération des clés ou de révocation de certificats. Un contrôle multi-utilisateur est également requis pour la génération des clés de l'AC, tel que décrit dans la section 6.2.2. Sous réserve des dispositions de la section 5.2.1, une seule personne peut accomplir toutes les autres tâches associées aux rôles de l'AC.

5.2.3 Identification et authentification pour chaque rôle

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'identité et les autorisations de chaque membre du personnel de l'AC doivent être vérifiées avant que ces personnes : 1. soient incluses dans la liste de contrôle d'accès au site de l'AC; 2. soient incluses dans la liste de contrôle d'accès qui contrôle l'accès physique au système de l'AC; 3. se voient délivrer un certificat pour l'exécution de leur rôle dans l'AC; 4. se voient attribuer un compte dans le système de l'ICP, lorsqu'un tel compte est nécessaire. Tout tel certificat ou compte, à l'exception du certificat de signature de l'AC : a) doit être attribuable directement à une seule personne; b) ne doit être partagé avec aucune autre personne; c) ne doit pas être utilisé à des fins autres que celles qui sont prévues pour l'exécution des tâches attribuées au personnel de l'AC à qui le certificat ou le compte concerné a été associé. L'AC doit mettre en œuvre ces exigences grâce aux logiciels de l'AC et du système d'exploitation et à des contrôles procéduraux.

5.2.4 Rôles qui nécessitent la séparation des tâches

L'AC doit mettre en œuvre une séparation des tâches à l'égard des fonctions critiques de l'AC, conformément à la section 5.2.1 (Rôles de confiance).

5.3 Contrôles du personnel

L'AC doit s'assurer que le personnel, à l'exception des employés du gouvernement du Canada, qui accomplit des tâches dans l'exploitation de l'AC ou d'une AE, conclut un contrat d'emploi ou reconnaît autrement les termes et conditions de sa participation. L'AC doit s'assurer que les termes et conditions d'emploi comprennent une clause exigeant que ce personnel ne divulgue pas d'informations sensibles touchant la sécurité de l'AC ou d'informations privées tel que défini dans la section 9.4.2.

L'AC ne doit pas assigner de tâches à des personnels pouvant provoquer un conflit d'intérêt avec leurs tâches dans l'AC ou l'AE.

5.3.1 Qualifications, expérience et habilitation de sécurité

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	L'AC doit s'assurer que tout le personnel qui accomplit des fonctions de l'AC et de l'AE possède les connaissances, l'expérience et les qualifications nécessaires pour s'acquitter de ses tâches. L'AC doit s'assurer que tout le personnel associé à l'exploitation de l'AC a subi avec succès une vérification approfondie de la fiabilité.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
	L'AC doit s'assurer que tout le personnel qui exploite une autorité d'enregistrement automatisé ou un logiciel de l'AE aux fins de la gestion en ligne des entités a subi avec succès au moins une vérification approfondie de la fiabilité.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit s'assurer que tout le personnel qui accomplit des fonctions de l'AC et de l'AE possède les connaissances, l'expérience et les qualifications nécessaires pour s'acquitter de ses tâches. L'AC doit s'assurer que tout le personnel associé à l'exploitation de l'AC possède la cote de sécurité Secret. L'AC doit s'assurer que tout le personnel qui exploite une autorité d'enregistrement automatisé ou un logiciel d'AE pour la gestion en ligne des entités a subi avec succès au moins une vérification approfondie de la fiabilité, qui doit comprendre une vérification des empreintes digitales et une vérification du crédit.

5.3.2 Procédures de vérification des antécédents

Toutes les vérifications des antécédents doivent être effectuées conformément à la Politique du gouvernement sur la sécurité.

5.3.3 Formation

L'AC doit s'assurer que tout le personnel reçoit la formation appropriée. Cette formation doit porter sur des sujets pertinents comme les exigences en matière de sécurité, les responsabilités opérationnelles et les procédures connexes.

5.3.4 Fréquence et exigences du recyclage

L'AC doit examiner et actualiser son programme de formation au moins une fois par année afin de tenir compte des modifications apportées au système de l'AC.

5.3.5 Fréquence et séquence de rotation des emplois

Aucune exigence n'est stipulée.

5.3.6 Sanctions pour des actions non autorisées

En cas d'actions non autorisées réelles ou présumées de la part d'une personne qui exécute des tâches relatives au fonctionnement de l'AC ou d'une AE, l'AC doit suspendre l'accès de cette personne au système de l'AC.

5.3.7 Exigences pour les entrepreneurs indépendants

L'AC doit s'assurer que le personnel contractuel satisfait aux mêmes exigences de sécurité du personnel en ce qui concerne la nomination, la formation et la vérification des antécédents, afin que ces exigences soient identiques aux exigences applicables aux employés de l'AC.

5.3.8 Documentation fournie au personnel

L'AC doit remettre aux personnels de l'AC, des AE ainsi qu'aux PRD les présentes PC, les dispositions pertinentes de l'EPC ainsi que les lois, les politiques ou les contrats qui sont pertinents pour leur poste.

5.4 Procédures de journalisation à des fins d'audit

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée. Il n'est pas nécessaire de tenir à jour de journal d'audit pour ce niveau d'assurance.

5.4.1 Types d'événements journalisés

L'AC doit s'assurer qu'elle est capable d'enregistrer ou de faire enregistrer dans des fichiers journaux d'audit tous les événements relevant de la sécurité du système de l'AC, et notamment ceux qui concernent les routeurs, les pare-feu, les annuaires et les serveurs qui hébergent des logiciels de l'AC et de l'AE. Toutes les fonctions d'audit de la sécurité du système d'exploitation de l'AC et des applications de l'AC doivent être activées.

Ces événements comprennent notamment :

1. Le démarrage et l'arrêt du système;
2. Le démarrage et l'arrêt de l'application de l'AC;
3. Les tentatives de création, d'effacement ou d'établissement des mots de passe, ou de modification des droits système de l'utilisateur maître de l'ICP, des responsables de la sécurité de l'ICP et des administrateurs de l'ICP;
4. Les modifications aux détails ou aux clés de l'AC;
5. Les changements apportés aux politiques de création des certificats (par exemple la période de validité);
6. Les tentatives de connexion et de déconnexion;
7. Les tentatives non autorisées d'accès réseau au système de l'AC;
8. Les tentatives non autorisées d'accès aux fichiers du système;
9. La génération des clés de l'AC et des entités subordonnées;
10. La création et la révocation des certificats;
11. Les tentatives d'initialisation, de suppression, d'activation et de désactivation des abonnés, ainsi que les tentatives de mise à jour et de récupération de leurs clés;
12. Les opérations échouées de lecture et d'écriture dans l'annuaire des certificats et des LCR.

Tous les journaux, qu'ils soient électroniques ou manuels, doivent indiquer la date et l'heure de l'événement ainsi que l'identité de l'entité qui a provoqué l'événement.

L'AC doit également recueillir, électroniquement ou manuellement, des informations sur la sécurité, non générées par le système de l'AC, par exemple :

1. Les journaux des accès physiques;
2. La maintenance et les modifications de la configuration du système, telles qu'elles sont définies dans l'EPC;
3. Les changements dans le personnel de l'AC;
4. Les rapports sur les anomalies et les compromissions;
5. Les renseignements concernant la destruction des informations sensibles;
6. Les versions actuelles et antérieures de toutes les politiques de certification;
7. Les versions actuelles et antérieures des énoncés des pratiques de certification;
8. Les rapports d'évaluation des vulnérabilités;

9. Les rapports d'évaluation des menaces et des risques;
10. Les rapports de certification et d'accréditation de l'AC;
11. Les rapports d'inspection de conformité;
12. Les versions actuelles et antérieures des accords d'utilisation et des autres documents que l'abonné a accepté de respecter (par exemple les recopies d'écran Web pertinentes utilisées pour l'enregistrement dans l'IPC).

L'AC doit indiquer dans l'EPC les informations qui doivent être journalisées.

Afin de faciliter le processus décisionnel, tous les accords et toute la correspondance portant sur les services de l'AC doivent être recueillis et regroupés, électroniquement ou manuellement, dans un seul endroit.

5.4.2 Fréquence de traitement des journaux d'audit

NIVEAU D'ASSURANCE	SIGNATURE NUMERIQUE CONFIDENTIALITE
Assurance de base	L'AC doit s'assurer que tous les événements significatifs sont expliqués dans un récapitulatif du journal d'audit et que le personnel de l'AC examine les journaux d'audit au moins **une fois aux deux (2) semaines**. Cet examen consiste à vérifier que le journal n'a pas été altéré, puis à inspecter toutes ses entrées. Le personnel de l'AC doit examiner plus en profondeur toutes les « alertes » ou les anomalies dans les journaux. L'AC doit indiquer dans l'EPC qui est responsable de l'examen des journaux d'audit et de la réalisation du récapitulatif de ces derniers. L'AC doit examiner les journaux manuels et électroniques connexes, y compris ceux des AE, lorsqu'une action est jugée suspecte. L'AC doit documenter les mesures qui sont prises à la suite de ces examens.
Assurance moyenne	L'AC doit s'assurer que tous les événements significatifs sont expliqués dans un récapitulatif du journal d'audit et que le personnel de l'AC examine les journaux d'audit au moins **une fois par semaine**. Cet examen consiste à vérifier que le journal n'a pas été altéré, puis à inspecter toutes ses entrées. Le personnel de l'AC doit examiner plus en profondeur toutes les « alertes » ou les anomalies dans les journaux. L'AC doit indiquer dans l'EPC qui est responsable de l'examen des journaux d'audit et de la réalisation du récapitulatif de ces derniers. L'AC doit examiner les journaux manuels et électroniques connexes, y compris ceux des AE, lorsqu'une action est jugée suspecte. L'AC doit documenter les mesures qui sont prises à la suite de ces examens.
Assurance élevée	L'AC doit s'assurer que tous les événements significatifs sont expliqués dans un récapitulatif du journal d'audit et que le personnel de l'AC examine les journaux d'audit au moins **une fois par jour**. Cet examen consiste à vérifier que le journal n'a pas été altéré, puis à inspecter toutes ses entrées. Le personnel de l'AC doit examiner plus en profondeur toutes les « alertes » ou les anomalies dans les journaux. L'AC doit indiquer dans l'EPC qui est responsable de l'examen des journaux d'audit et de la réalisation du récapitulatif de ces derniers. L'AC doit examiner les journaux manuels et électroniques connexes, y compris ceux des AE, lorsqu'une action est jugée suspecte. L'AC doit documenter les mesures qui sont prises à la suite de ces examens.

5.4.3 Période de rétention des journaux d'audit

L'AC doit conserver ses journaux d'audit sur place pendant au moins deux (2) mois, et par la suite conserver les journaux d'audit générés par le logiciel de l'ICP de la manière décrite dans la section 5.5.

5.4.4 Protection des journaux d'audit

L'AC doit protéger le système électronique des journaux d'audit et les informations d'audit saisies électroniquement ou manuellement contre toute consultation, modification, suppression ou destruction non autorisée.

5.4.5 Procédures de sauvegarde des journaux d'audit

L'AC doit sauvegarder ou copier, si en format papier, tous les journaux d'audit et les récapitulatifs d'audit.

5.4.6 Système de collecte des informations d'audit (internes ou externes)

L'AC doit indiquer dans l'EPC ses systèmes de collecte des informations d'audit.

5.4.7 Notification du sujet ayant causé un événement

Lorsqu'un événement est journalisé par le système de collecte des informations d'audit, l'AC se réserve le droit de ne pas avertir la personne, le rôle, l'appareil ou l'application qui a causé l'événement en question.

5.4.8 Évaluation des vulnérabilités

Dans le processus d'audit, les événements sont journalisés, en partie, afin de surveiller les vulnérabilités du système. L'AC doit s'assurer qu'une évaluation des vulnérabilités est effectuée, examinée et révisée à la suite d'un examen de ces événements surveillés, et elle doit prendre les mesures qui s'imposent pour minimiser les vulnérabilités détectées dans le système dès que cela est raisonnablement possible.

5.5 Archivage des documents

En plus d'être soumises aux stipulations des sous-sections suivantes, les informations conservées ou sauvegardées par l'AC peuvent être assujetties à d'autres exigences d'archivage, conformément à la *Loi sur les Archives nationales du Canada*, à d'autres lois pertinentes et aux politiques du GC.

5.5.1 Types de documents archivés

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée. À ce niveau d'assurance, l'archivage des documents n'est pas requis.
Assurance de base **Assurance moyenne** **Assurance élevée**	Les certificats, les certificats croisés et les certificats de l'AC (autosignés) conservés par l'AC, ainsi que les LAR et les LCR générées par l'AC doivent être gardés pendant au moins deux (2) ans après leur expiration. Les informations suivantes doivent être archivées : 1. Les journaux d'audit générés par le logiciel de l'AC de l'ICP; 2. Les ententes avec les abonnés; 3. Les documents portant sur de l'information d'identification et

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
	d'authentification; 4. Les journaux des accès physiques; 5. Les opérations de maintenance et les changements apportés à la configuration du système, tels qu'ils sont définis dans l'EPC; 6. Les changements dans le personnel de l'AC; 7. Les rapports sur les anomalies et les compromissions; 8. Les informations concernant la destruction des informations sensibles; 9. Les versions actuelles et antérieures de toutes les politiques de certification; 10. Les versions actuelles et antérieures des énoncés des pratiques de certification; 11. Les rapports d'évaluation des vulnérabilités; 12. Les rapports d'évaluation des menaces et des risques; 13. Les rapports d'inspection de conformité; 14. Les rapports d'accréditation et de certification de l'AC; 15. Les versions actuelles et antérieures des accords d'utilisation et des autres documents que l'abonné a accepté de respecter (par exemple les recopies des écrans Web pertinents utilisés dans le cadre du processus d'enregistrement dans l'ICP); 16. La documentation qui indique tous les personnels qui ont reçu une formation reliée à l'AC ainsi que le niveau de formation obtenu.

5.5.2 Période de rétention des documents archivés

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée. L'archivage des documents n'est pas requis à ce niveau d'assurance.
Assurance de base **Assurance moyenne** **Assurance élevée**	Les certificats, les certificats croisés et les certificats de l'AC (autosignés) conservés par l'AC, ainsi que les LAR et les LCR générées par l'AC, doivent être gardés pendant au moins deux (2) ans après leur expiration. Les informations d'audit, décrites dans la section 5.4, doivent être conservées pendant une période qui doit être définie dans l'énoncé des pratiques de certification. Les clés de confidentialité privées qui sont sauvegardées par l'AC doivent être archivées pendant une période de dix ans. L'AC doit archiver tous les mots de passe et les clés nécessaires pendant une période de temps permettant à l'AC de s'acquitter de ses responsabilités.

5.5.3 Protection des documents archivés

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée. L'archivage des documents n'est pas requis à ce niveau d'assurance.
Assurance de base **Assurance moyenne** **Assurance élevée**	Les clés de confidentialité privées sauvegardées par l'AC doivent être protégées à un niveau de protection physique et cryptographique au moins égal à celui qui est en place dans le site de l'AC. Une deuxième copie de tous les documents conservés ou sauvegardés doit être stockée dans un endroit autre que le site de l'AC et doit être protégée par des moyens de sécurité physique uniquement, ou par une combinaison de moyens de protection physique et cryptographique. Tout site secondaire doit offrir une protection adéquate contre les menaces environnementales comme la température, l'humidité et le magnétisme.

5.5.4 Procédures de sauvegarde des documents archivés

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée. L'archivage des documents n'est pas requis à ce niveau d'assurance.
Assurance de base **Assurance moyenne** **Assurance élevée**	Une deuxième copie de tous les documents conservés ou sauvegardés doit être stockée dans un lieu autre que le site de l'AC.

5.5.5 Horodatage des documents

Aucune exigence n'est stipulée.

5.5.6 Système de collecte des informations archivées (internes ou externes)

Aucune exigence n'est stipulée.

5.5.7 Procédures d'obtention et de vérification des informations archivées

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée. L'archivage des documents n'est pas requis à ce niveau d'assurance.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit vérifier l'intégrité des copies de sauvegarde une fois aux six (6) mois, ainsi que l'intégrité des documents stockés hors site une fois par année, et elle doit décrire le processus de vérification de cette intégrité.

5.6 Renouvellement des clés

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit indiquer dans l'EPC : 1. la période pendant laquelle les clés de l'abonné peuvent être renouvelées avant la date d'expiration du certificat, pourvu que celui-ci n'ait pas été révoqué; 2. le processus grâce auquel l'AC, une AE ou l'abonné peut lancer le renouvellement des clés. Le renouvellement automatique des clés est autorisé. Les abonnés sans clés valides doivent être réauthentifiés de la même manière que lors de l'enregistrement initial. Les clés de l'AC sont renouvelées automatiquement à la fréquence définie dans la section 6.3.2 des présentes politiques de certification.

5.7 Compromission et reprise après sinistre

5.7.1 Procédures de traitement des incidents et des compromissions

Compromission de la clé de l'AC

À la suite de la compromission de la clé de signature numérique privée de l'AC et avant sa régénération, l'AC doit immédiatement :

1. notifier toutes les parties comme pour la révocation du certificat public de l'AC;
2. demander la révocation des certificats croisés délivrés à l'AC;
3. révoquer tous les certificats délivrés au moyen de cette clé.

Après avoir réglé les problèmes qui ont conduit à la compromission de la clé, l'AC peut générer une nouvelle paire de clés de signature de l'AC et réémettre les certificats à toutes les entités, en s'assurant que toutes les LCR et les LAR sont signées au moyen de cette nouvelle clé.

L'AC doit indiquer dans l'EPC ou dans un document publié et dans les accords appropriés comment elle procédera pour avertir de la compromission de sa clé de signature.

Révocation du certificat public de l'AC

Lorsqu'il est nécessaire de révoquer le certificat de signature numérique de l'AC, l'AC doit immédiatement avertir :

1. l'AGP de l'ICP du GC;
2. toutes les AC auxquelles elle a délivré un certificat croisé;
3. toutes ses AE;
4. tous les abonnés;
5. tous les parrains ministériels et les PRD;
6. tous les propriétaires responsables d'application.

L'AC doit publier le numéro de série du certificat dans une LAR appropriée et révoquer tous les certificats croisés signés avec le certificat de signature numérique de l'AC révoqué.

Après avoir réglé les problèmes qui ont conduit à la compromission de la clé, l'AC peut générer une nouvelle paire de clés de signature de l'AC et réémettre les certificats à toutes les entités, en s'assurant que toutes les LCR et les LAR sont signées au moyen de cette nouvelle clé.

L'AC doit indiquer dans l'EPC ou dans un document publié et dans les accords appropriés comment elle procédera pour avertir de la compromission de sa clé de signature.

5.7.2 Corruption des ressources informatiques, des logiciels ou des données

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit indiquer dans l'EPC ou dans un autre document approprié les procédures qui décrivent les étapes qui doivent être entreprises en cas de corruption ou de perte des ressources informatiques, des logiciels ou des données. Lorsqu'un référentiel n'est pas sous le contrôle de l'AC, l'AC doit s'assurer que toute entente ou accord conclu avec ce référentiel prévoit que ce dernier établira et documentera les procédures à suivre en cas de corruption ou de perte des ressources informatiques, des logiciels ou des données du référentiel.

5.7.3 Procédures en cas de compromission de la clé privée d'une entité

Voir la section 4.9.

5.7.4 Capacité de poursuivre les activités après un sinistre

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit élaborer et tenir à jour un plan de continuité des activités décrivant les étapes qui doivent être entreprises afin de rétablir une installation sécurisée à la suite d'un sinistre naturel ou d'une autre nature. Le plan de continuité des activités doit prendre en compte de ce qui suit : 1. La définition des rôles et des personnalités des personnes responsables de l'exécution des diverses parties du plan; 2. Les conditions d'activation du plan, avec une description de la marche à suivre avant l'activation de ce dernier; 3. Les procédures d'urgence, avec une description des actions qui doivent être entreprises à la suite d'un incident qui met en danger les activités ou la vie humaine; 4. Les procédures de secours, avec une description des actions qui doivent être entreprises afin de transférer les activités essentielles ou les services de soutien dans un autre endroit, et de rétablir les processus opérationnels dans les délais requis; 5. Les procédures de reprise, avec une description des actions qui doivent

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
	être entreprises afin de rétablir les activités normales; 6. Un calendrier de maintenance, précisant comment et quand le plan sera testé, ainsi que le processus d'actualisation du plan; 7. Les activités de sensibilisation et de formation, destinées à faire comprendre les processus de continuité des activités et à garantir l'efficacité permanente de ces derniers. Lorsqu'un référentiel n'est pas sous le contrôle de l'AC, l'AC doit s'assurer que toute entente ou accord avec ce référentiel prévoit que ce dernier établisse et documente un plan de continuité des activités.

5.8 Cessation des activités de l'AC ou d'une AE

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.

L'AC, lorsqu'elle met fin à ses activités ou leur apporte des modifications importantes, doit avertir l'AGP de l'ICP du GC ainsi que toutes les entités à l'égard desquelles elle a délivré des certificats et toutes les AC avec lesquelles elle a établi une certification croisée; cet avis doit être fourni avant ou immédiatement après la cessation des activités ou le changement majeur dans ces dernières.

Lorsque l'AC met fin à ses activités, les clés privées de l'AC qui ont déjà été utilisées ou qui pourraient être utilisées pour poursuivre les opérations cryptographiques de l'AC doivent être révoquées (pour motif de cessation des activités) et détruites conformément à la section 6.2.10 (Méthode de destruction des clés privées). Une LCR et une LAR finales doivent être générées et publiées.

Lorsque l'AC met fin à ses activités, elle doit prévoir la conservation de ses documents par un gardien autorisé, y compris deux copies :

1. des certificats;
2. des clés privées de confidentialité (le cas échéant);
3. des certificats croisés;
4. des certificats autosignés par l'AC;
5. des LCR et des LAR;
6. des informations d'audit décrites dans la section 5.4;
7. des autres documents qui ont été archivés tel que décrit dans la section 5.5,

conformément aux exigences d'archivage stipulées dans les présentes politiques de certification.

L'AC doit également prévoir la conservation de toutes les données (par exemple les mots de passe) nécessaires pour garantir que les documents de l'AC sont exploitables (par exemple que les données chiffrées peuvent être déchiffrées ultérieurement au besoin).

Le transfert sécurisé doit être réalisé conformément à la section 5.1.8 (Sauvegarde hors site).

6. CONTRÔLES TECHNIQUES DE SÉCURITÉ

L'AC doit sécuriser toutes ses opérations au moyen de mécanismes comme l'authentification forte et le chiffrement quand l'accès se fait sur un réseau partagé.

6.1 Génération et installation des paires de clés

Le GC ne stipule aucune exigence concernant les cérémonies de clés racines pour les AC du GC.

6.1.1 Génération des paires de clés

Génération des clés de l'AC

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	L'AC doit s'assurer que la génération des clés de l'AC est réalisée au moyen d'un algorithme approuvé par l'AGP de l'ICP du GC.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit s'assurer que la génération des clés de l'AC : 1. est réalisée par du personnel dans des rôles de confiance, sous double contrôle au minimum; 2. est réalisée au moyen d'un appareil qui satisfait aux exigences de la section 6.2.1 ou à des exigences supérieures; 3. est réalisée au moyen d'un algorithme approuvé par l'AGP de l'ICP du GC. L'AC doit documenter ses procédures de génération des clés de l'AC et générer une preuve auditable démontrant que les procédures documentées ont été respectées.

Génération des clés de l'AE

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	L'AC doit s'assurer que la génération des clés de l'AE est réalisée au moyen d'un algorithme approuvé par l'AGP de l'ICP du GC.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit s'assurer que la génération des clés de l'AE : 1. est réalisée au moyen d'un appareil qui satisfait aux exigences de la section 6.2.1 ou à des exigences supérieures; 2. est réalisée au moyen d'un algorithme approuvé par l'AGP de l'ICP du GC.

Génération des clés de l'abonné

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Chaque paire de clés de signature numérique doit être générée au moyen d'un algorithme approuvé par l'AGP de l'ICP du GC.	Chaque paire de clés de confidentialité doit être générée au moyen d'un algorithme approuvé par l'AGP de l'ICP du GC.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Lorsqu'une paire de clés est générée pour le compte d'un utilisateur potentiel, l'entité ou le processus qui a généré les clés doit détruire sa copie de la paire de clés de manière sûre après avoir confié les clés à la garde de l'abonné potentiel. Les paires de clés des entités finales, à l'exception de celles de l'AC, doivent être générées au moyen d'un module cryptographique logiciel ou matériel conformément à la section 6.2.1.

6.1.2 Fourniture de la clé privée à l'abonné

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Lorsque l'abonné potentiel ne génère pas la clé de signature privée, l'AC doit stocker cette dernière de manière que seul l'abonné potentiel puisse y accéder.	Lorsque l'abonné potentiel ne génère pas la clé de déchiffrement privée, l'AC doit stocker cette dernière de manière que seul l'abonné potentiel puisse y accéder.

6.1.3 Fourniture de la clé publique à l'émetteur du certificat

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Lorsque l'AC ne génère pas la clé de vérification publique, l'AC doit prévoir sa fourniture à l'AC, de manière sûre, tel que documenté dans l'EPC.	Lorsque l'AC ne génère pas la clé de chiffrement publique, l'AC doit prévoir sa fourniture à l'AC, de manière sûre, tel que documenté dans l'EPC.

6.1.4 Fourniture de la clé publique de l'AC aux parties utilisatrices

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	La clé de vérification publique de l'AC doit être fournie aux parties utilisatrices de manière sûre, afin d'assurer l'authenticité, tel que décrit dans l'EPC.

6.1.5 Tailles des clés

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	L'AC doit utiliser un algorithme RSA 1 024 ou 2 048 bits pour sa propre paire de clés de signature. Lorsque c'est possible et lorsque l'AC utilise un algorithme sur 2 048 bits pour sa propre paire de clés de signature, les entités finales doivent utiliser un algorithme RSA 2 048 bits pour leurs paires de clés. Lorsque l'AC utilise un algorithme RSA 1 024 bits pour sa propre paire de clés de signature ou lorsque cela n'est pas possible, les entités finales doivent utiliser un algorithme RSA 1 024 bits pour leurs paires de clés.
Assurance de base **Assurance moyenne**	L'AC doit utiliser un algorithme RSA 2 048 bits pour sa propre paire de clés de signature. Les AC doivent utiliser des clés RSA 2 048 bits lorsqu'elles signent des certificats et des LCR à compter d'une date déterminée par l'AGP. Toutes les clés d'abonnés dans les certificats émis après une date déterminée par l'AGP doivent être au moins des clés RSA 2 048 bits.
Assurance élevée	L'AC doit utiliser un algorithme RSA 2 048 bits pour sa propre paire de clés de signature. Les entités finales doivent également utiliser un algorithme RSA 2 048 bits pour leurs paires de clés.

6.1.6 Génération et contrôle de la qualité des paramètres des clés publiques

Aucune exigence n'est stipulée.

6.1.7 Utilisations des clés (champ keyUsage selon x509v3)

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.	Aucune exigence n'est stipulée.
Assurance de base	Les clés peuvent être utilisées pour assurer l'authentification et l'intégrité des données et à l'appui de la non-répudiation.	Les clés peuvent être utilisées pour l'échange et l'établissement des clés utilisées pendant la session et pour assurer la confidentialité des données.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance moyenne **Assurance élevée**	Les clés de signature de l'AC sont les seules clés qu'on peut utiliser pour signer les certificats et les LCR. Le champ KeyUsage du certificat doit être utilisé conformément au profil des champs de base et des champs d'extension des LCR et des certificats X.509 de l'ICP du GC.	Le champ KeyUsage du certificat doit être utilisé conformément au profil des champs de base et des champs d'extension des LCR et des certificats X.509 de l'ICP du GC.

6.2 Protection des clés privées et contrôles techniques des modules cryptographiques

6.2.1 Normes et contrôles des modules cryptographiques

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne**	Tout module cryptographique utilisé par l'AC, le personnel de l'AC, les AE et les abonnés doit satisfaire aux exigences suivantes : 1. Toutes les opérations de génération de la clé de signature numérique de l'AC, de stockage de la clé de signature numérique de l'AC et de signature des certificats doivent être réalisées au moyen d'un module cryptographique matériel homologué FIPS 140-1 ou FIPS 140-2 niveau 3 ou fournissant un niveau équivalent de fonctionnalités et d'assurance. 2. Toutes les autres opérations cryptographiques de l'AC doivent être réalisées au moyen d'un module cryptographique homologué FIPS 140-1 ou FIPS 140-2 niveau 2 ou fournissant un niveau équivalent de fonctionnalités et d'assurance. 3. Les opérations de signature et de génération de la clé de signature numérique des AE doivent être réalisées au moyen d'un module cryptographique matériel homologué au moins FIPS 140-1 ou FIPS 140-2 niveau 1 ou fournissant un niveau équivalent de fonctionnalités et d'assurance. Les opérations d'enregistrement automatisé peuvent être réalisées au moyen d'un module cryptographique logiciel homologué au moins FIPS 140-1 ou FIPS 140-2 niveau 1 ou fournissant un niveau équivalent de fonctionnalités et d'assurance, pourvu que l'AC soit convaincue que la sécurité physique du logiciel est adéquate. Toutes les autres opérations cryptographiques de l'AE doivent être réalisées au moyen de modules cryptographiques homologués FIPS 140-1 ou FIPS 140-2 niveau 1 ou fournissant un niveau équivalent de fonctionnalités et d'assurance. 4. Les entités finales doivent utiliser des modules cryptographiques homologués au moins FIPS 140-1 ou FIPS 140-2 niveau 1 ou fournissant un niveau équivalent de fonctionnalités et d'assurance. 5. Tous les cryptomodules doivent automatiquement se verrouiller après une période d'inactivité déterminée.

Assurance élevée	Tout module cryptographique utilisé par l'AC, le personnel de l'AC, les AR et les abonnés doit satisfaire aux exigences suivantes : 1. Toutes les opérations de génération de la clé de signature numérique de l'AC, de stockage de la clé de signature numérique de l'AC et de signature des certificats doivent être réalisées au moyen d'un module cryptographique matériel homologué FIPS 140-1 ou FIPS 140-2 niveau 3 ou fournissant un niveau équivalent de fonctionnalités et d'assurance. 2. Toutes les autres opérations cryptographiques de l'AC doivent être réalisées au moyen d'un module cryptographique homologué FIPS 140-1 ou FIPS 140-2 niveau 2 ou fournissant un niveau équivalent de fonctionnalités et d'assurance. 3. Les opérations de signature et de génération de la clé de signature numérique des AE doivent être réalisées au moyen d'un module cryptographique matériel homologué au moins FIPS 140-1 ou FIPS 140-2 niveau 2 ou fournissant un niveau équivalent de fonctionnalités et d'assurance. Les opérations d'enregistrement automatisé peuvent être réalisées au moyen d'un module cryptographique logiciel homologué au moins FIPS 140-1 ou FIPS 140-2 niveau 1 ou fournissant un niveau équivalent de fonctionnalités et d'assurance, pourvu que l'AC soit convaincue que la sécurité physique du logiciel est adéquate. Toutes les autres opérations cryptographiques de l'AE doivent être réalisées au moyen de modules cryptographiques homologués FIPS 140-1 ou FIPS 140-2 niveau 2 ou fournissant un niveau équivalent de fonctionnalités et d'assurance. 4. Les entités finales doivent utiliser des modules cryptographiques homologués au moins FIPS 140-1 ou FIPS 140-2 niveau 2 ou fournissant un niveau équivalent de fonctionnalités et d'assurance. 5. Tous les cryptomodules doivent automatiquement se verrouiller après une période d'inactivité déterminée.

6.2.2 Contrôle multi-personne des clés privées (n sur m)

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Les opérations de génération des clés de l'AC doivent faire l'objet d'un contrôle multi-personne. Deux personnes, dont l'une accomplit les tâches associées au rôle de l'utilisateur maître de l'ICP, doivent participer ou être présentes. La gestion du cycle de vie ou la délivrance des clés à des rôles de confiance doivent faire l'objet d'un contrôle multi-personne. Deux personnes, dont une accomplit les tâches associées au rôle du responsable de la sécurité de l'ICP, doivent participer ou être présentes.	On peut permettre à l'abonné de réaliser de façon sûre les opérations de récupération ou de révocation de ses propres clés. Lorsque ces opérations ne sont pas effectuées par l'abonné lui-même, la récupération de la clé privée d'une entité finale doit faire l'objet d'un contrôle multi-personne. Deux personnes, dont l'une est un responsable de la sécurité de l'ICP ou une AE, doivent participer ou être présentes.

6.2.3 Séquestre des clés privées

L'AC ne doit pas participer au séquestre des clés privées par une tierce partie.

6.2.4 Sauvegarde des clés privées

Stockage, sauvegarde et récupération des clés de l'AC

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit s'assurer que les clés privées de l'AC demeurent confidentielles et que leur intégrité est maintenue. En particulier : 1. La clé de signature privée de l'AC doit être conservée et utilisée dans un appareil cryptographique sécurisé qui satisfait aux exigences de la section 6.2.1; 2. La clé de signature privée de l'AC peut être exportée par tout moyen approuvé par le CST, d'un appareil cryptographique dans un autre appareil cryptographique qui satisfait aux exigences de la section 6.2.1; 3. Lorsqu'elle se trouve à l'extérieur de l'appareil de création de la signature, la clé de signature privée de l'AC doit être chiffrée; 4. La clé de signature privée de l'AC doit être sauvegardée, stockée et récupérée sous le même contrôle multi-personne que la clé originale, et la copie de sauvegarde doit être conservée de manière sûre dans le site de réserve de l'AC; 5. Lorsque les clés de l'AC sont conservées dans un module matériel de traitement des clés dédiées, des contrôles d'accès doivent être mis en place afin de garantir qu'il est impossible d'accéder aux clés à l'extérieur du module matériel.

L'AC doit indiquer dans l'EPC ses procédures de sauvegarde des clés.

Sauvegarde des clés de l'abonné

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Une entité peut sauvegarder sa propre clé de signature numérique privée. Dans ce cas, la clé doit être copiée et conservée sous forme chiffrée et protégée à un niveau au moins égal à celui qui est stipulé pour la version primaire de la clé. Lorsque les clés de signature numérique sont stockées dans un	Normalement, l'AC doit sauvegarder les clés de déchiffrement privées de ses entités. À titre exceptionnel, l'AC peut ne pas sauvegarder les clés de déchiffrement privées de certaines de ses entités. Une entité peut réaliser une copie de sauvegarde de ses propres clés de déchiffrement privées.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
	référentiel central, l'AC peut sauvegarder les clés de signature numérique privées des abonnées, pourvu que ces clés soient adéquatement protégées contre le contournement des mécanismes de sécurité (accès par déchiffrement par l'abonné uniquement).	Les clés sauvegardées doivent être conservées sous forme chiffrée et protégées à un niveau au moins égal à celui qui est stipulé à l'égard de la version primaire de la clé.

6.2.5 Archivage des clés privées

Reportez-vous à la section 5.5.

6.2.6 Transfert des clés privées en direction ou en provenance d'un module cryptographique

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Lorsqu'une clé de signature privée n'est pas générée dans le module cryptographique de l'entité, elle doit être entrée dans ce module de façon sûre.	Lorsqu'une clé de déchiffrement privée n'est pas générée dans le module cryptographique de l'entité, elle doit être entrée dans ce module de façon sûre.

6.2.7 Stockage des clés privées dans un module cryptographique

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Les clés privées doivent être stockées dans un ESP.

6.2.8 Méthode d'activation des clés privées

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance de base **Assurance moyenne** **Assurance élevée**	Une entité doit être authentifiée auprès de l'ESP avant l'activation de la clé privée. L'AC doit s'assurer que des règles régissant l'utilisation des mots de passe sont en place et qu'elles nécessitent l'utilisation de mots de passe forts pour accéder à un ESP. L'AGP de l'ICP du GC peut approuver d'autres méthodes d'authentification pour l'activation des clés privées.

6.2.9 Méthode de désactivation des clés privées

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Le module cryptographique doit automatiquement désactiver la clé privée après une période d'inactivité prédéterminée. Lorsque les clés privées sont désactivées, elles doivent être effacées de la mémoire avant que celle-ci soit désallouée, et elles doivent être conservées sous forme chiffrée uniquement. Tout l'espace disque dans lequel les clés ont été stockées doit être effacé par superposition d'écriture avant que cet espace soit réalloué au système d'exploitation.

6.2.10 Méthode de destruction des clés privées

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Lorsque le titulaire d'une clé privée a fini de l'utiliser, il doit détruire de façon sûre toutes les copies de cette clé dans la mémoire de l'ordinateur et dans l'espace disque partagé. Dans le cas des modules cryptographiques logiciels, cette opération peut être réalisée en supprimant l'ESP, puisque les clés sont conservées dans un ESP sous forme chiffrée. Dans le cas des modules cryptographiques matériels, cette opération peut probablement être effectuée en lançant une commande de « remise à zéro ». La destruction physique des jetons matériels ne devrait pas être requise.

6.2.11 Évaluation des modules cryptographiques

Conformément à la section 6.2.1 (Normes et contrôles des modules cryptographiques).

6.3 Autres aspects de la gestion des paires de clés

6.3.1 Archivage des clés publiques

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit conserver tous les certificats de clé publique de vérification de signature numérique qu'elle génère.	L'AC doit conserver tous les certificats de clé publique de chiffrement qu'elle génère.

6.3.2 Périodes opérationnelles des certificats et périodes d'utilisation des paires de clés

	ASSURANCE RUDIMENTAIRE		ASSURANCE DE BASE — ASSURANCE MOYENNE – ASSURANCE ÉLEVÉE	
Clé/certificat	**Longueur de la clé en bits**	**Période de validité maximale**	**Longueur de la clé en bits**	**Période de validité maximale**
Clé de signature privée de l'AC	1 024 ou 2 048	36 mois	2 048	96 mois
Certificat et clé de vérification publique de l'AC	1 024 ou 2 048	72 mois	2 048	240 mois
Clé de signature privée d'une entité finale	1 024 ou 2 048	36 mois	1 024 ou 2 048	38 mois
Certificat et clé de vérification publique d'une entité finale	1 024 ou 2 048	36 mois	1 024 2 048	72 mois 144 mois
Certificat et clé de chiffrement publique d'une entité finale	1 024 ou 2 048	36 mois	1 024 2 048	72 mois 144 mois
Clé de déchiffrement privée d'une entité finale	1 024 ou 2 048	Pas de délai d'expiration	1 024 ou 2 048	Pas de délai d'expiration

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Toutes les données d'activation doivent être uniques et imprévisibles. Les clés et les données d'initialisation peuvent être générées en masse et elles doivent être conservées de façon sûre par l'AC avant leur distribution. Sur réception des données d'initialisation, l'abonné doit se servir de ces dernières en temps voulu.

6.4.2 Protection des données d'activation

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	Les données utilisées pour l'initialisation d'une entité doivent être protégées contre toute utilisation non autorisée par une combinaison de mécanismes de contrôle d'accès cryptographique et physique. L'environnement de sécurité personnel des entités doit être protégé contre toute utilisation non autorisée par des mécanismes cryptographiques. Les données d'activation, en conjonction avec tous les autres contrôles d'accès, doivent posséder un niveau de résistance approprié aux clés ou aux données qui doivent être protégées. Lorsque des mots de passe sont utilisés, l'AC doit s'assurer que les applications ou le système de l'ICP appliquent une politique de mots de passe forts. Le niveau de protection doit être suffisant pour décourager un attaquant motivé disposant de ressources importantes. Lorsqu'on utilise un système de mots de passe réutilisables, le mécanisme doit comprendre une fonction qui verrouille temporairement le compte à la suite d'un nombre prédéterminé de tentatives de connexion infructueuses. L'entité doit pouvoir changer son mot de passe en tout temps.

6.4.3 Autres aspects des données d'activation

Aucune exigence n'est stipulée.

6.5 Contrôles de sécurité informatique

6.5.1 Exigences techniques propres à la sécurité informatique

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne**	Le serveur de l'AC doit comprendre les fonctionnalités de sécurité suivantes : 1. Contrôle d'accès aux services de l'AC et aux rôles de l'ICP; 2. Séparation des tâches pour les rôles de l'ICP; 3. Identification et authentification des rôles de l'ICP et des identités associées; 4. Contrôles de la réutilisation des objets ou séparation pour l'accès à la mémoire vive (RAM) de l'AC; 5. Le cas échéant, utilisation de moyens cryptographiques pour les communications de la session et la sécurité de la base de données; 6. Archivage de l'historique et des données d'audit de l'AC et des entités finales; 7. Audit des événements relevant de la sécurité; 8. Validation automatique et périodique de l'intégrité de la base de données de l'AC; 9. Mécanismes de chemin de confiance pour l'identification et l'authentification des rôles de l'ICP et des identités associées; 10. Mécanismes de récupération des clés et du système de l'AC; 11. Durcissement du système d'exploitation de l'AC. Ces fonctionnalités peuvent être fournies par le système d'exploitation, ou grâce à une combinaison du système d'exploitation, du logiciel de l'AC de l'ICP et de moyens de protection physiques.
Assurance élevée	Le serveur de l'AC, en plus de posséder les fonctionnalités de sécurité requises pour l'assurance de base ou l'assurance moyenne, doit également appliquer à l'égard des processus critiques pour la sécurité des limites d'intégrité de domaine. Ces fonctionnalités peuvent être fournies par le système d'exploitation ou par une combinaison du système d'exploitation, du logiciel de l'AC de l'ICP et de moyens de protection physiques.

6.5.2 Évaluation de la sécurité informatique

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance de base **Assurance moyenne** **Assurance élevée**	Le CST ou tout autre laboratoire tiers accrédité doit évaluer les éléments de l'AC qui sont critiques du point de vue de la sécurité.

6.6 Contrôles techniques du cycle de vie

6.6.1 Contrôles sur le développement du système

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base	L'AC doit utiliser un logiciel d'AC qui a été conçu et développé selon une méthode de développement structurée. Le processus de conception et de développement du logiciel de l'AC doit être supporté par une vérification tierce de la conformité au processus. Le matériel ou le logiciel acheté doit être livré ou fourni dans un contenant scellé, emballé sous plastique ou d'une autre manière fiable et il doit être installé par du personnel formé adéquatement.
Assurance moyenne	L'AC doit utiliser un logiciel d'AC qui a été conçu et développé selon une méthode de développement structurée. Le processus de conception et de développement doit être supporté par une vérification tierce de la conformité au processus et des évaluations courantes des menaces et des risques afin d'influer sur la conception des mesures de protection de la sécurité et de minimiser les risques résiduels. Le matériel ou le logiciel acheté doit être livré ou fourni dans un contenant scellé, emballé sous plastique ou d'une autre manière fiable et il doit être installé par du personnel formé adéquatement.
Assurance élevée	L'AC doit utiliser un logiciel d'AC qui a été conçu et développé selon une méthode de développement structurée. Le processus de conception et de développement doit comporter suffisamment de documentation pour supporter la vérification tierce de la conformité au processus, l'évaluation tierce de la sécurité des composantes de l'AC et des évaluations courantes des menaces et des risques afin d'influer sur la conception des mesures de protection de la sécurité et de minimiser les risques résiduels. Le matériel ou le logiciel acheté doit être livré ou fourni dans un contenant scellé, emballé sous plastique ou d'une autre manière fiable et il doit être installé par du personnel formé adéquatement.

6.6.2 Contrôles de gestion de la sécurité

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base	Le matériel et le logiciel de l'AC doivent être dédiés uniquement à la réalisation des tâches de l'AC. Il ne doit y avoir aucune autre application, périphérique, connexion réseau ou composante logicielle qui ne fasse pas partie des activités de l'AC. L'AC doit indiquer dans l'EPC ses politiques et procédures qui visent à empêcher le chargement de logiciels malveillants dans les équipements de l'AC. Les logiciels de l'AC et de l'AE ainsi que les logiciels d'enregistrement automatisé doivent faire l'objet d'une vérification afin de détecter les programmes malveillants lors de leur première utilisation et périodiquement par la suite. L'AC doit utiliser un processus de gestion de la configuration pour l'installation et la maintenance courante du système de l'AC. Le logiciel de l'AC, lors de son premier chargement, doit comporter une méthode permettant à l'AC de vérifier que le logiciel installé dans le système : 1. émane du développeur du logiciel; 2. n'a pas été modifié avant son installation; 3. correspond bien à la version que l'on compte utiliser. L'AC doit fournir un mécanisme permettant de vérifier périodiquement l'intégrité de la base de données de l'AC. L'AC doit également établir des mécanismes et des politiques pour contrôler et surveiller la configuration du système de l'AC. Lors de l'installation, et au moins aux **deux semaines**, l'intégrité de la base de données de l'AC doit être validée.
Assurance moyenne	Le matériel et le logiciel de l'AC doivent être dédiés uniquement à la réalisation des tâches de l'AC. Il ne doit y avoir aucune autre application, périphérique, connexion réseau ou composante logicielle qui ne fasse pas partie des activités de l'AC. L'AC doit indiquer dans l'EPC ses politiques et procédures qui visent à empêcher le chargement de logiciels malveillants dans les équipements de l'AC. Les logiciels de l'AC et de l'AE ainsi que les logiciels d'enregistrement automatisé doivent faire l'objet d'une vérification afin de détecter les programmes malveillants lors de leur première utilisation et périodiquement par la suite. L'AC doit utiliser une méthode formelle de gestion de la configuration pour l'installation et la maintenance courante du système de l'AC. Le logiciel de l'AC, lors de son premier chargement, doit comporter une méthode permettant à l'AC de vérifier que le logiciel installé dans le système : 1. émane du développeur du logiciel; 2. n'a pas été modifié avant son installation; 3. correspond à la version que l'on compte utiliser. L'AC doit fournir un mécanisme permettant de vérifier périodiquement l'intégrité de la base de données de l'AC. L'AC doit également établir des

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
	mécanismes et des politiques pour contrôler et surveiller la configuration du système de l'AC. Lors de l'installation, et au moins **une fois par semaine**, l'intégrité de la base de données de l'AC doit être validée.
Assurance élevée	Le matériel et le logiciel de l'AC doivent être dédiés uniquement à la réalisation des tâches de l'AC. Il ne doit y avoir aucune autre application, périphérique, connexion réseau ou composante logicielle qui ne fasse pas partie des activités de l'AC. L'AC doit indiquer dans l'EPC ses politiques et procédures qui visent à empêcher le chargement de logiciels malveillants dans les équipements de l'AC. Les logiciels de l'AC et de l'AE ainsi que les logiciels d'enregistrement automatisé doivent faire l'objet d'une vérification afin de détecter les programmes malveillants lors de leur première utilisation et périodiquement par la suite. L'AC doit utiliser une méthode formelle de gestion de la configuration pour l'installation et la maintenance courante du système de l'AC. Le logiciel de l'AC, lors de son premier chargement, doit comporter une méthode permettant à l'AC de vérifier que le logiciel installé dans le système : 1. émane du développeur du logiciel; 2. n'a pas été modifié avant son installation; 3. correspond à la version que l'on compte utiliser. L'AC doit fournir un mécanisme permettant de vérifier périodiquement l'intégrité de la base de données de l'AC. L'AC doit également établir des mécanismes et des politiques pour contrôler et surveiller la configuration du système de l'AC. Lors de l'installation, et au moins **une fois aux 24 heures**, l'intégrité de la base de données de l'AC doit être validée.

6.7 Contrôles de sécurité réseau

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit s'assurer que des contrôles de sécurité sont établis afin d'assurer l'intégrité et la disponibilité de l'AC à travers tout réseau ouvert ou à usage général auquel elle est connectée. Cette protection doit comprendre l'installation d'un ou de plusieurs appareils configurés pour autoriser uniquement les protocoles et, au choix de l'AC, les commandes requises pour les activités de l'AC. Tout logiciel réseau présent doit être nécessaire au fonctionnement de l'AC. L'AC doit indiquer dans son EPC ces protocoles et, au besoin, les commandes requises pour le fonctionnement de l'AC.

6.8 Horodatage

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Aucune exigence n'est stipulée.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC peut fournir aux abonnés ou aux titulaires de certificat, ou voir à ce que leur soit fournie, la possibilité d'horodater leurs transactions.

7. PROFILS DES CERTIFICATS, DES LCR ET OCSP

7.1 Profil des certificats

7.1.1 Numéro de version

L'AC doit émettre des certificats X.509 version 3 ou ultérieure, pourvu que leur utilisation soit approuvée par l'AGP de l'ICP du GC.

Le logiciel de l'entité finale de l'ICP doit supporter tous les champs X.509 de base (ceux qui ne sont pas des extensions).

NOM DU CHAMP	DESCRIPTION
Signature	Signature de l'AC pour authentifier le certificat
Issuer	Nom de l'AC
Validity	Dates d'activation et d'expiration du certificat
Subject	Nom distinctif de l'abonné
Subject Public Key Information	Clé ID de l'algorithme
Version	Version du certificat X.509
Serial Number	Numéro de série unique du certificat

7.1.2 Extensions du certificat

Les règles d'inclusion, d'attribution d'une valeur et de traitement des extensions sont définies dans des profils. Les extensions des certificats utilisées par des certificats émis conformément aux présentes politiques de certification doivent se conformer aux parties applicables du profil des champs et des extensions des certificats X.509 et des LCR de l'ICP du GC.

L'AC doit diffuser son profil des champs de base et des champs extensions des certificats X.509 et des LCR sur un site Web, et fournir son adresse aux abonnés.

Les extensions privées critiques doivent être interopérables au sein de leur communauté d'utilisation prévue.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Lorsque des extensions privées sont utilisées, elles peuvent être identifiées dans l'EPC.
Assurance de base **Assurance moyenne** **Assurance élevée**	Lorsque des extensions privées sont utilisées, elles doivent être identifiées dans l'EPC.

7.1.3 Identificateurs d'objet des algorithmes

L'AC et les entités finales doivent utiliser uniquement des algorithmes de chiffrement et de condensé approuvés par l'AGP de l'ICP du GC, et ce conformément aux délais approuvés par l'AGP.

L'AC doit utiliser, et les entités finales doivent supporter, les algorithmes symétriques suivants :

<table>
<tr><th colspan="3">CHIFFREMENT</th></tr>
<tr><td>Assurance rudimentaire</td><td colspan="2">Aucune exigence n'est stipulée.</td></tr>
<tr><td rowspan="3">Assurance de base
Assurance moyenne
Assurance élevée</td><td>Algorithme</td><td>Commentaires</td></tr>
<tr><td>Triple DES</td><td>L'option des « trois clés indépendantes » est l'option privilégiée. L'option à deux clés est également acceptable, lorsque la clé utilisée pour le chiffrement final est identique à la clé utilisée pour le premier chiffrement.

L'option à une seule clé n'est pas acceptable, puisqu'elle réduit la sécurité à celle d'un algorithme DES à passage unique.

La cryptopériode de n'importe quelle clé ne doit pas dépasser sept (7) jours.</td></tr>
<tr><td>CAST 5/80 ou CAST 5/128</td><td>Les modes de fonctionnement acceptables sont identiques à ceux qui ont été spécifiés à l'origine pour DES.

La cryptopériode de n'importe quelle clé ne doit pas dépasser vingt-quatre (24) heures.</td></tr>
</table>

La liste des algorithmes que doivent utiliser toutes les entités de l'ICP peut être modifiée sans que cela n'entraîne la publication d'une nouvelle politique de certification ou un changement dans l'OID de la PC.

Lorsqu'un changement quelconque est apporté à un algorithme approuvé, l'AC doit s'assurer que les abonnés sont mis au courant des modifications apportées à la liste des algorithmes approuvés en vue d'une utilisation à l'intérieur du GC. L'AC doit indiquer dans son EPC la manière dont elle entend donner un tel avis de changement.

7.1.4 Forme des noms

Chaque DN doit prendre la forme d'une chaîne imprimable X.501.

7.1.5 Contraintes sur les noms

Lorsqu'elle est utilisée, l'extension name constraints doit être garnie et traitée tel que décrit dans le profil des champs et des extensions des certificats X.509 et des LCR de l'ICP du GC.

7.1.6 Identificateur d'objet des politiques de certification

L'AC doit s'assurer que les OID des politiques pertinentes figurent dans les certificats qu'elle émet.

7.1.7 Utilisation de l'extension policyConstraint

Lorsqu'elle est utilisée, l'extension policyConstraint doit être garnie et traitée tel que décrit dans le profil des champs et des extensions des certificats X.509 et des LCR de l'ICP du GC.

7.1.8 Syntaxe et sémantique des qualificateurs de politique

Lorsqu'elle est utilisée, l'extension policyQualifiers doit être garnie et traitée tel que décrit dans le profil des champs et des extensions des certificats X.509 et des LCR de l'ICP du GC.

7.1.9 Sémantique de traitement des extensions critiques des certificats

Les extensions critiques, lorsqu'elles sont marquées, doivent être interprétées tel que défini dans le profil des champs et des extensions des certificats X.509 et des LCR de l'ICP du GC.

7.2 Profil des LCR

7.2.1 Numéro de version

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Lorsqu'elle met en œuvre des LCR, l'AC doit publier des LCR et des LAR X.509 version deux (2) ou ultérieure, pourvu que leur utilisation soit approuvée par l'AGP de l'ICP du GC. L'AC peut indiquer dans son EPC l'utilisation des extensions supportées par l'AC, ses AE et ses entités finales.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC doit publier des LCR et des LAR X.509 version deux (2) ou ultérieure, pourvu que leur utilisation soit approuvée par l'AGP de l'ICP du GC. L'AC doit indiquer dans son EPC l'utilisation des extensions supportées par l'AC, ses AE et ses entités finales.

7.2.2 LCR et extensions des entrées des LCR

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Lorsque des LCR sont mises en œuvre, le logiciel d'ICP de toutes les entités doit traiter correctement toutes les extensions des LCR indiquées dans le profil des champs et des extensions des certificats X.509 et des LCR de l'ICP du GC. L'AC doit indiquer dans son EPC l'utilisation des extensions supportées par l'AC, ses AE et ses entités finales.
Assurance de base **Assurance moyenne** **Assurance élevée**	Le logiciel d'ICP de toutes les entités doit correctement traiter toutes les extensions des LCR indiquées dans le profil des champs et des extensions des certificats X.509 et des LCR de l'ICP du GC. L'AC doit indiquer dans son EPC l'utilisation des extensions supportées par l'AC, ses AE et ses entités finales.

7.3 Profil OCSP

7.3.1 Numéro de version

Lorsque l'utilisation de serveurs OCSP est approuvée par l'AGP de l'ICP du GC ou par une AGP d'un ministère, l'AC doit se conformer au profil OCSP de l'ICP du GC.

7.3.2 Extensions OCSP

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Lorsque l'utilisation de serveurs OCSP est approuvée par l'AGP de l'ICP du GC ou par une AGP ministérielle, les logiciels d'ICP de toutes les entités doivent traiter correctement toutes les extensions OCSP indiquées dans le profil OCSP de l'ICP du GC. L'AC peut indiquer dans son EPC l'utilisation des extensions supportées par l'AC, ses AE et ses entités finales.
Assurance de base **Assurance moyenne** **Assurance élevée**	Lorsque l'utilisation de serveurs OCSP est approuvée par l'AGP de l'ICP du GC ou par une AGP ministérielle, les logiciels d'ICP de toutes les entités doivent traiter correctement toutes les extensions OCSP indiquées dans le profil OCSP de l'ICP du GC. L'AC doit indiquer dans son EPC l'utilisation des extensions supportées par l'AC, ses AE et ses entités finales.

8. AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

Une inspection de conformité vise à déterminer si l'AC satisfait aux exigences établies par les présentes politiques de certification et les EPC associés.

Une inspection de conformité de l'AC sera effectuée aux termes et conditions établis par l'AGP de l'ICP du GC, ou par une AGP ministérielle dans le cas d'une AC ministérielle. Dans le cadre du processus de certification croisée avec le PIFC, l'AC doit fournir à l'AGP de l'ICP du GC les résultats de toute inspection de conformité effectuée dans le cadre de ce processus. Les rapports des inspections de conformité ne doivent pas être rendus publics, sauf lorsque cela est exigé par la loi en vertu d'une autorité judiciaire, d'une exigence législative explicite ou d'une entente.

8.1 Fréquence ou circonstances des évaluations

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	L'AC doit établir, à la satisfaction de toute AC avec laquelle elle a conclu une certification croisée, qu'elle se conforme intégralement aux exigences de la présente politique : 1. Avant la certification croisée initiale avec une AC de l'ICP du GC; 2. Au moins aux trois ans par la suite.
Assurance de base	L'AC doit faire l'objet d'une inspection de conformité au moins une fois par année. Un inspecteur qualifié provenant de l'extérieur de l'AC doit effectuer une (1) inspection sur **cinq** (5) de l'AC. L'AGP de l'ICP du GC peut en tout temps demander une inspection de conformité de l'AC par un organisme externe. L'AGP de l'ICP du GC peut, à sa discrétion et en tout temps, demander au sous-ministre responsable de l'AC de faire effectuer une inspection de conformité par un organisme externe au ministère. L'AC doit certifier une fois par année à l'AGP de l'ICP du GC qu'elle s'est, en tout temps pendant la période concernée, conformée aux exigences des présentes politiques de certification, et elle doit fournir les motifs pour lesquels elle ne s'est pas conformée à ces politiques de certification et indiquer les périodes de non-conformité éventuelles.
Assurance moyenne **Assurance élevée**	L'AC doit faire l'objet d'une inspection de conformité au moins une fois par année. Un inspecteur qualifié provenant de l'extérieur de l'AC doit effectuer une (1) inspection sur **trois** (3) de l'AC. L'AGP de l'ICP du GC peut en tout temps demander une inspection de conformité de l'AC par un organisme externe. L'AGP de l'ICP du GC peut, à sa discrétion et en tout temps, demander au sous-ministre responsable de l'AC de faire effectuer une inspection de conformité par un organisme externe au ministère. L'AC doit certifier une fois par année à l'AGP de l'ICP du GC qu'elle s'est, en tout temps pendant la période concernée, conformée aux exigences des présentes politiques de certification, et elle doit fournir les motifs pour lesquels elle ne s'est pas conformée à ces politiques de certification et indiquer les périodes de non-conformité éventuelles.

8.2 Identité et qualifications de l'évaluateur

L'inspecteur doit faire la preuve de sa compétence dans le domaine des inspections de conformité, et il doit bien connaître les exigences que l'AGP de l'ICP du GC impose à la délivrance et à la gestion des certificats émis conformément aux présentes politiques de certification.

8.3 Relations de l'évaluateur avec l'entité évaluée

L'inspecteur doit être indépendant de la gestion ou du fonctionnement de l'AC.

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

8.4 Sujets couverts par l'évaluation

L'inspection de conformité doit porter au minimum sur les points suivants :

1. L'EPC décrit-il avec suffisamment de détails les pratiques (techniques, procédures, personnel) de l'AC requises en vertu des présentes politiques de certification?
2. L'AC applique-t-elle ces pratiques relatives aux techniques, procédures et personnel, et s'y conforme-t-elle?
3. Le gestionnaire de référentiel, les AE et les ALE appliquent-ils les pratiques établies par l'AC en matière de techniques, de procédures et de personnel, et s'y conforment-ils?

L'inspecteur peut consulter les propriétaires responsables d'application pour déterminer les applications, les procédures et les pratiques pertinentes susceptibles d'avoir un effet sur l'inspection.

L'AGP de l'ICP du GC peut étendre la portée d'une inspection de conformité, aux conditions qu'elle juge appropriées.

8.5 Mesures prises à la suite du constat de lacunes

Les résultats de l'inspection seront soumis à l'autorité d'accréditation de l'AC et à l'AGP de l'ICP du GC. Lorsque des irrégularités sont constatées, l'AC présente un rapport à l'autorité d'accréditation et à l'AGP de l'ICP du GC concernant les mesures que l'AC entend prendre suite au rapport d'inspection.

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE CONFIDENTIALITÉ
Assurance rudimentaire	Lorsqu'une AC ne prend pas les mesures appropriées suite au rapport d'inspection, l'autorité d'accréditation peut : 1. indiquer les irrégularités, mais permettre à l'AC de poursuivre ses activités jusqu'à la prochaine inspection prévue; 2. permettre à l'AC de poursuivre ses activités pour une période maximale de **quatre-vingt-dix** (90) jours, dans l'attente que des corrections soient apportées aux problèmes, avant la révocation; ou 3. révoquer le certificat de l'AC. Lorsque l'autorité d'accréditation ne prend pas les mesures qui s'imposent, l'AGP de l'ICP du GC peut révoquer la certification croisée de l'AC avant le PIFC. Le choix de ces mesures dépendra de la gravité des irrégularités.

Assurance de base **Assurance moyenne** **Assurance élevée**	Lorsqu'une AC ne prend pas les mesures appropriées suite au rapport d'inspection, l'autorité d'accréditation peut : 1. indiquer les irrégularités, mais permettre à l'AC de poursuivre ses activités jusqu'à la prochaine inspection prévue; 2. permettre à l'AC de poursuivre ses activités pour une période maximale de **trente** (30) jours, dans l'attente que des corrections soient apportées aux problèmes, avant la révocation; 3. réduire le niveau d'assurance de la certification croisée avec le PIFC; ou 4. révoquer le certificat de l'AC. Lorsque l'autorité d'accréditation ne prend pas les mesures appropriées, l'AGP de l'ICP du GC peut : 1. réduire le niveau d'assurance de la certification croisée avec le PIFC; ou 2. révoquer le certificat croisé de l'AC avec le PIFC. Le choix de ces mesures dépend de la gravité des irrégularités.

8.6 Communication des résultats

Les résultats de l'inspection doivent être considérés comme des données sensibles et ils ne doivent être divulgués pour aucune autre raison que les fins de l'inspection ou lorsque cela est requis par une entente ou par une loi, en vertu d'une autorité judiciaire ou d'une exigence législative explicite.

9. AUTRES QUESTIONS ET QUESTIONS JURIDIQUES

9.1 Redevances

9.1.1 Redevances pour la délivrance ou le renouvellement d'un certificat

La facturation de redevances pour la délivrance et la gestion des certificats et des LCR est assujettie aux politiques et aux dispositions législatives appropriées. L'AC ne doit pas facturer de redevances aux abonnés ou aux parties utilisatrices sans l'approbation de l'AGP de l'ICP du GC.

Lorsque des redevances sont facturées, ces redevances doivent faire l'objet d'un avis, et aucune redevance ne doit être facturée tant que les abonnés et les parties utilisatrices n'ont pas été notifiés, de la manière appropriée, et qu'ils n'ont pas eu l'occasion de renoncer à recevoir les services de l'AC.

La facturation de redevances en relation avec l'inscription dans un programme ou l'utilisation des services de ce dernier dépasse la portée de la présente politique. Ces redevances sont déterminées et mises en œuvre par le personnel autorisé du ministère ou de l'organisme.

9.1.2 Redevances pour l'accès aux certificats

Aucune exigence n'est stipulée.

9.1.3 Redevances pour l'accès aux informations sur l'état ou la révocation

Aucune exigence n'est stipulée.

9.1.4 Redevances pour d'autres services

Aucune exigence n'est stipulée.

9.1.5 Politique de remboursement

Aucune exigence n'est stipulée.

9.2 Responsabilité financière

Lorsque l'AC conclut un marché pour la prestation de services d'AC quelconques, elle doit s'assurer que le fournisseur de services présente une preuve satisfaisante de sa responsabilité financière et, le cas échéant, renonce à toute immunité législative.

9.2.1 Couverture de l'assurance

Aucune exigence n'est stipulée.

9.2.2 Autres actifs

Aucune exigence n'est stipulée.

9.2.3 Couverture de l'assurance ou de la garantie pour les entités finales

Aucune exigence n'est stipulée.

9.3 Confidentialité des informations d'entreprise

9.3.1 Portée des informations confidentielles

Les informations confidentielles d'entreprise d'une organisation sont considérées privées aux fins de la protection de l'information.

9.3.2 Informations ne relevant pas des informations confidentielles

Aucune exigence n'est stipulée.

9.3.3 Responsabilité à l'égard de la protection des informations confidentielles

Les informations confidentielles d'entreprise associées à la délivrance des certificats conformément aux présentes politiques de certification sont considérées particulièrement sensibles et doivent par conséquent être marquées PROTÉGÉ B.

9.4 Confidentialité des informations personnelles

9.4.1 Plan de confidentialité

La sensibilité des informations privées détenues par les ministères en rapport avec les certificats délivrés conformément aux présentes politiques de certification varie et elle est déterminée par rapport :

1. Aux lois et règlements pertinents, notamment la *Loi sur la protection des renseignements personnels*, la *Loi sur l'accès à l'information* et la *Loi sur les Archives nationales du Canada*;
2. Aux politiques de sécurité pertinentes du gouvernement;
3. Aux politiques pertinentes du gouvernement sur la protection de la vie privée.

9.4.2 Informations considérées comme privées

Types d'informations privées

Les informations privées sont (1) des informations identifiables sur une personne et (2) des informations d'entreprise confidentielles d'une organisation.

Collecte permise des informations privées

L'AC ne doit pas recueillir d'informations privées à une autre fin que celle de la délivrance et de la gestion des certificats au personnel d'un programme, à l'AC ou à n'importe quel fournisseur de services d'AC, à une AE ou à une entité finale. L'AC ne doit pas recueillir plus d'informations que cela n'est nécessaire à cette fin.

Les ministères peuvent demander des renseignements, des justificatifs ou des autorisations additionnels pour l'inscription dans un programme particulier, en plus de ceux qui sont prévus par la politique de certification.

Possibilité pour le propriétaire de corriger ses informations privées

Le propriétaire des informations privées, ou une organisation désignée le cas échéant, peut corriger les inexactitudes ou demander que des corrections soient apportées aux informations privées qu'il a fournies, et ce en tout temps. L'AC et n'importe quelle AE désigneront une personne qui sera responsable de recevoir les demandes de correction des informations privées reliées à l'ICP, et publiera les coordonnées d'une personne contact dans son site Web, ou de n'importe quelle autre manière appropriée dans des circonstances particulières.

Les informations privées détenues par les ministères ou les organismes, en rapport avec les programmes pour lesquels des certificats ont été délivrés conformément aux présentes politiques de certification, sont assujetties aux lois et aux politiques pertinentes qui régissent ces programmes. Les modalités de correction de ces informations seront déterminées par le gestionnaire opérationnel du programme concerné.

9.4.3 Informations non considérées comme privées

Les informations qui concernent la révocation ou la suspension d'un certificat, et notamment le code du motif, peuvent être incluses dans une entrée de la LCR. Les certificats et les LCR ne sont pas considérés comme des informations privées aux fins des présentes politiques de certification.

9.4.4 Responsabilité à l'égard de la protection des informations privées

Les informations privées associées à la délivrance de certificats conformément aux présentes politiques de certification sont considérées particulièrement sensibles et par conséquent doivent être marquées PROTÉGÉ B.

9.4.5 Avis et consentement d'utilisation des informations privées

L'AC doit s'assurer que toute demande d'un certificat devant être délivré par l'AC comporte une formulation visant à obtenir le consentement du demandeur d'utiliser et de divulguer des informations privées, tel que décrit dans les présentes politiques de certification et dans tout accord connexe.

Utilisation permise des informations privées

L'AC doit se servir des informations privées recueillies par elle ou par l'AE uniquement pour la délivrance et la gestion d'un certificat conformément aux présentes politiques de certification.

L'emploi des informations privées recueillies par les ministères et les organismes, en rapport avec des programmes qui doivent utiliser des certificats délivrés conformément aux présentes politiques de certification, est déterminé par les gestionnaires opérationnels de programme du ministère ou de l'organisme, qui sont responsables du programme ou du service concerné, et peut varier selon l'application.

9.4.6 Divulgation dans le cadre d'un processus judiciaire ou administratif

L'AC ou n'importe quelle AE doit divulguer les informations privées recueillies aux fins de la délivrance et de la gestion des certificats, uniquement aux responsables de l'application de la loi ou lorsqu'on le leur demande dans le cadre d'une procédure judiciaire. Cette divulgation exige la réception (1) d'une ordonnance judiciaire; (2) le consentement du propriétaire des informations privées; ou (3) une autorisation législative explicite.

9.4.7 Autres circonstances de la divulgation des informations

Distribution permise des informations privées

Sous réserve des dispositions des sections 9.4.5 et 9.4.6 ainsi que des limitations et des autorisations imposées par la *Loi sur la protection des renseignements personnels* et les autres lois, règlements et politiques pertinents, l'AC et n'importe quelle AE peut distribuer des informations privées uniquement aux personnels des ministères ou des organismes qui en ont besoin aux fins de la délivrance et de la gestion des certificats.

L'AC ou n'importe quelle AE peut communiquer des informations privées si, d'après elle, il existe une situation où la vie est menacée.

Toute communication d'informations privées propres à un programme est assujettie aux lois et aux politiques pertinentes.

9.5 Droits de propriété intellectuelle

Tous les droits, titres et intérêts dans tous les droits de propriété intellectuelle ou associés à ces politiques de certification, LCR, LAR, noms distinctifs, accords de service, certificats et clés publiques de l'AC ainsi qu'aux certificats des entités finales (les éléments matériels), y compris toutes les modifications et les améliorations qui leur sont apportées, sont et doivent demeurer la propriété exclusive du GC.

Les abonnés et les parties utilisatrices peuvent se servir de ces éléments matériels uniquement aux fins de se conformer aux présentes politiques de certification. Toute autre utilisation, commerciale ou non commerciale, est strictement interdite. La PC peut être copie et distribuée, pourvu que les avis de copyright ou les autres avis de propriété, lorsqu'il y en a, soient conservés, ou qu'un avis équivalent soit fourni concernant leur origine et leur propriété.

Tout logiciel fourni en rapport avec l'utilisation des éléments matériels demeure la propriété du GC ou de ses concédants de licence tiers. L'utilisation de ce logiciel doit se faire conformément aux termes de la licence de logiciel pertinente.

9.6 Déclarations et garanties

9.6.1 Déclarations et garanties de l'AC

NIVEAU D'ASSURANCE	SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Assurance rudimentaire	L'AC est responsable de la création et de la signature des certificats qui lient les abonnés, le personnel de l'AC et (lorsque cela est permis) les autres AC à leurs clés publiques de vérification. L'AC peut également générer des paires de clés de signature numérique pour une entité finale lorsqu'elle utilise un processus d'enregistrement automatisé.	L'AC est responsable de la création et de la signature des certificats qui lient les abonnés et le personnel de l'AC à leurs clés publiques de chiffrement. L'AC doit également générer les paires de clés de confidentialité pour une entité finale lorsque cela est nécessaire.
Assurance de base **Assurance moyenne** **Assurance élevée**	L'AC est responsable : a) de la création et de la signature des certificats qui lient les abonnés, le personnel de l'AC et (lorsque cela est permis) les autres AC à leurs clés publiques de vérification; b) de faire connaître l'état des certificats dans des LCR et des LAR. L'AC peut également générer des paires de clés de signature numérique pour une entité finale lorsqu'elle utilise un processus d'enregistrement automatisé.	L'AC est responsable : a) de la création et de la signature des certificats qui lient les abonnés et le personnel de l'AC à leurs clés publiques de chiffrement; b) de faire connaître l'état des certificats dans des LCR et des LAR. L'AC doit également générer les paires de clés de confidentialité pour une entité finale lorsque cela est nécessaire.

Les autres dispositions de la section 9.6.1 concernent uniquement une AC qui délivre des certificats à un ou plusieurs niveaux d'assurance, de l'assurance de base à l'assurance élevée.

L'AC doit :

1. fonctionner dans le but d'émettre et de gérer les certificats des abonnés, du personnel de l'AC, des AE et des gestionnaires de référentiels, et d'émettre et de gérer des certificats croisés conformément aux présentes politiques de certification, aux EPC pertinents, aux lois pertinentes du Canada ainsi qu'aux politiques du gouvernement du Canada;
2. élaborer un EPC détaillé décrivant toutes les pratiques, les procédures et les exigences requises pour se conformer aux présentes politiques de certification;
3. s'assurer que toutes les AE et les gestionnaires de référentiels qui agissent pour son compte fonctionnent en conformité avec les présentes PC et les EPC pertinents;
4. s'assurer que des accords ou des ententes pertinents qui décrivent les droits, les privilèges et les obligations des parties concernées ont été conclus avec :
   (a) les abonnés, pour les certificats qui leur sont délivrés ou qui sont délivrés à leur demande;
   (b) toutes les autres parties qui accomplissent des fonctions pour le compte de l'AC.
5. présenter, dans un document public, l'information dont les demandeurs de certificats peuvent avoir besoin pour demander la délivrance, la suspension ou la révocation d'un certificat;
6. fournir aux abonnés et aux parties utilisatrices un avis décrivant leurs droits, privilèges et obligations respectifs concernant l'utilisation des clés, des certificats, du matériel ou du logiciel fournis par l'AC;
7. avertir les abonnés lorsqu'un certificat à leur égard :
   (a) est délivré;
   (b) est suspendu;
   (c) est révoqué.
8. indiquer l'adresse de la LCR dans les certificats délivrés conformément aux présentes politiques;
9. faire connaître à toutes les parties intéressées les procédures appliquées par l'AC pour l'expiration, la suspension, la révocation et le renouvellement des certificats;
10. mettre à la disposition des abonnés ou des parties utilisatrices, conformément aux présentes PC, les informations concernant les révocations;
11. se servir de sa clé de signature privée uniquement pour signer des certificats et des LCR, et à aucune autre fin;
12. établir des procédures visant à garantir que le personnel de l'AC associé aux rôles de l'ICP (p. ex., l'utilisateur maître de l'ICP, les responsables de la sécurité de l'ICP et les administrateurs de l'ICP) est tenu responsable des actions qu'il accomplit et qu'il existe une preuve permettant d'associer une action à la personne qui l'a accomplie;
13. s'assurer que le personnel de l'AC utilise les clés privées émises pour la conduite des tâches de l'AC uniquement à cette fin;
14. sous réserve des lois et des politiques pertinentes du Canada, s'assurer que l'information détenue par l'AC ou pour le compte de l'AC est gardée au Canada;
15. sauf mention expresse du contraire, la publication d'un certificat dans un référentiel constitue une certification de la part de l'AC, et un avis à l'abonné ou à une partie utilisatrice qui peut consulter le certificat dans le référentiel, que l'information qui figure dans le certificat a été vérifiée conformément aux présentes politiques de certification;

16. établir des mécanismes pour minimiser les périodes de temps pendant lesquelles les services de l'AC ne sont pas disponibles aux entités finales;
17. intégrer un avis de limitation de responsabilité dans les certificats qu'elle crée. En raison des limites d'espace imposées au certificat, cet avis doit être restreint à la formulation suivante : « Limited Liability. See CP.-Responsabilité limitée. Voir PC. ».

SIGNATURE NUMÉRIQUE	CONFIDENTIALITÉ
Lorsque la technologie employée l'exige (p. ex., profils d'itinérance), l'AC doit placer les clés de signature privées de l'abonné en stockage protégé.	Lorsque la technologie employée l'exige (p. ex., profils d'itinérance), l'AC doit placer les clés de déchiffrement privées de l'abonné en stockage protégé.

9.6.2 Déclarations et garanties de l'AE

L'AE doit :

1. se conformer aux dispositions pertinentes des présentes PC et de l'EPC, ainsi qu'aux termes et conditions de tout accord ou entente avec l'AC;
2. faire connaître aux demandeurs la procédure de demande, y compris la procédure d'initialisation des certificats;
3. sauf dans le cas du niveau d'assurance rudimentaire, avant la délivrance du certificat, identifier et authentifier les identités des demandeurs qui désirent devenir des abonnés et, lorsqu'elle présente à l'AC les renseignements pour ces demandes, certifier à l'AC que cela a été fait conformément aux exigences des présentes politiques de certification;
4. faire connaître aux abonnés :
   (a) leurs droits, privilèges et obligations respectifs concernant l'utilisation des clés de l'ICP, des certificats, du matériel ou du logiciel fourni par l'AC;
   (b) les procédures de l'AC applicables à l'expiration, à la suspension, à la révocation et au renouvellement des clés et des certificats;
5. lorsque l'AC n'enregistre pas l'information, s'assurer, à des fins d'audit, qu'une trace est conservée des actions accomplies dans la réalisation des tâches de l'AE;
6. protéger les clés privées de l'AE conformément aux directives de l'AC.

Les AE peuvent supporter des processus d'enregistrement automatisé en ligne et hors ligne.

9.6.3 Déclarations et garanties de l'abonné

Une personne peut demander un certificat pour l'utiliser pour son propre compte ou pour le compte d'une autre entité (une application, un appareil, un rôle organisationnel ou une autre personne), pourvu qu'elle dispose d'une autorisation appropriée vérifiable. Dans ce cas, les obligations de l'abonné s'étendent à la personne autorisée à agir pour son compte.

L'abonné doit :

1. s'assurer que les renseignements présentés à l'AC ou à l'AE directement ou pour son compte sont complets et exacts;
2. se conformer aux termes :
   (a) de la politique d'utilisation de l'ICP par les employés, dans le cas des employés du GC;

(b) d'un accord d'abonnement ou d'un autre instrument ayant force exécutoire, à la satisfaction de l'AC;

3. utiliser les clés ou les certificats ou s'y fier uniquement aux fins permises par les présentes politiques de certification et pour aucune autre fin;
4. réaliser les opérations cryptographiques prévues au moyen du logiciel et du matériel appropriés;
5. protéger ses clés privées, ses mots de passe et ses jetons de clés (le cas échéant) de la manière établie dans les présentes politiques de certification ou tel qu'indiqué, et prendre toutes les mesures raisonnables pour empêcher leur perte, leur divulgation, leur modification ou leur utilisation non autorisée;
6. ne pas laisser son poste de travail sans surveillance lorsque la protection cryptographique est désactivée (c.-à-d. lorsque le NIP ou le mot de passe a été entré);
7. assumer ses responsabilités à l'égard de la protection des informations après leur déchiffrement ou leur vérification, tout particulièrement lorsque l'abonné choisit de rechiffrer l'information à des fins de stockage;
8. avertir immédiatement l'AC, de la manière indiquée par l'AC, en cas de compromission réelle ou présumée des clés privées de l'abonné, de son mot de passe ou de ses jetons de clés (le cas échéant);
9. en ce qui concerne l'utilisation à l'extérieur du Canada du matériel ou du logiciel contenant des éléments ou des produits cryptographiques, vérifier que :

   (a) l'importation ou l'utilisation de tels produits est permise dans un pays ou une juridiction particulière;

   (b) l'exportation de tels produits à partir Canada vers un autre pays ou une autre juridiction est permise.

9.6.4 Déclarations et garanties de la partie utilisatrice

La décision prise par une partie utilisatrice de se fier à un certificat peut être évaluée par la partie utilisatrice elle-même ou par une entité qui contrôle ou coordonne la façon dont les parties utilisatrices ou leurs applications se servent des certificats. Dans ce cas, les obligations de la partie utilisatrice s'étendent à l'entité qui contrôle ou coordonne l'utilisation du certificat.

La partie utilisatrice doit :

1) réaliser les opérations cryptographiques prévues au moyen du logiciel et du matériel appropriés;
2) avant de se fier à un certificat, vérifier l'état du certificat dans la LCR à jour appropriée ou dans le serveur OCSP, conformément aux exigences stipulées dans les sections 4.9.6 ou 4.9.10.

9.6.5 Déclarations et garanties des autres parties

Déclarations et garanties des organisations désignées

Lorsqu'une organisation (une « organisation désignée ») présente une demande de certificat destiné à être utilisé par une personne, un appareil, une application ou un rôle, l'organisation désignée, en plus de se conformer aux exigences de la section 9.6.3, doit également :

1. assumer l'entière responsabilité de l'exactitude et du caractère complet de tous les renseignements présentés à l'AC ou à l'AE, ainsi que de l'utilisation des clés, des certificats, du matériel ou du logiciel émis à ses abonnés par l'AC;
2. nommer et confirmer l'identité d'une ou de plusieurs personnes autorisées à agir pour son compte (les « personnes responsables désignées »);
3. par l'entremise des personnes responsables désignées, vérifier et communiquer à l'AC ou à une AE l'identité et les justificatifs des personnes qui doivent détenir des certificats pour leur propre utilisation individuelle ou pour une utilisation avec des appareils, des applications ou des rôles organisationnels dans l'organisation désignée;
4. certifier que tous les renseignements qui figurent dans ces certificats et toutes les demandes de services de l'AC sont exactes et complètes;
5. s'assurer que personne d'autre que l'abonné n'aura accès aux clés de signature privées dont il est responsable;
6. s'assurer que toutes les données d'activation associées aux environnements de sécurité personnels (ESP) de ces certificats demeurent confidentielles;
7. en ce qui concerne les certificats délivrés à l'égard d'un appareil, d'une application ou d'un rôle, s'assurer qu'une seule personne est responsable de ces certificats pendant une période de temps déterminée;
8. avertir l'AC ou une AE lorsque la relation de l'organisation désignée avec une ALE a changé de telle sorte que le certificat devrait être révoqué ou mis à jour, ou lorsqu'il y a un changement quelconque dans les informations de l'ALE ou l'autorisation d'agir pour le compte de l'organisation désignée;
9. documenter, détenir et produire sur demande des documents décrivant la situation de l'abonné et ses autorisations à des fins de vérification, lesdits documents liant une personne particulière à un certificat qui lui a été attribué, pendant la période pendant laquelle ce certificat est ainsi attribué;
10. s'assurer que les abonnés :
    (a) utilisent les clés ou les certificats ou s'y fient uniquement aux fins autorisées par les présentes politiques de certification ou tout autre accord ou entente que l'organisation désignée a pu conclure avec le GC;
    (b) réalisent les opérations cryptographiques prévues au moyen du logiciel et du matériel appropriés, tel qu'approuvé par l'AGP;
    (c) protègent les clés privées, les mots de passe et les jetons de clés (le cas échéant) confiés à leur garde de la manière prévue dans les présentes politiques de certification ou dans les directives, et prendre toutes les mesures raisonnables pour empêcher leur perte, leur divulgation, leur modification ou leur utilisation non autorisée;
    (d) avertissent immédiatement l'AC, de la manière prévue par l'AC, en cas de compromission réelle ou présumée des clés privées associées au certificat qu'elles détiennent.

NIVEAU D'ASSURANCE	EXIGENCES
Assurance rudimentaire	Les clés privées de l'abonné doivent être conservées de façon sûre dans un environnement de sécurité personnel (ESP). Une organisation désignée doit : a) utiliser de façon régulière et actualiser des mécanismes antivirus;

NIVEAU D'ASSURANCE	EXIGENCES
Assurance de base	b) actualiser les logiciels des postes de travail des clients; c) protéger les postes de travail des clients au moyen de services de pare-feu; d) assurer la gestion de la configuration des environnements clients afin de minimiser les vulnérabilités; e) mettre en œuvre une politique de mots de passe selon laquelle, au minimum, (i) les mots de passe système par défaut choisis par le fournisseur sont changés immédiatement; (ii) les mots de passe choisis par le fournisseur ne sont pas utilisés; (iii) les postes de travail des clients, dans la mesure du possible, comportent des comptes utilisateurs protégés par mots de passe; (iv) les mots de passe, lorsque c'est possible, comportent au moins huit caractères, avec une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.
Assurance moyenne **Assurance élevée**	Les clés privées de l'abonné doivent être conservées de façon sûre dans un ESP. Une organisation désignée doit certifier au propriétaire responsable de l'application qu'elle a pris des mesures appropriées pour : a) utiliser de façon régulière et actualiser des mécanismes antivirus; b) mettre en œuvre un politique de « correctifs de sécurité et de mise à jour du logiciel »; c) établir des services de pare-feu afin de protéger son environnement TI, et de façon plus précise ouvrir uniquement les ports requis pour ses activités et mettre en place un système de règles dans lequel tous les accès qui ne sont pas spécifiquement autorisés sont refusés; d) s'assurer que l'environnement TI de l'organisation et les utilisateurs des certificats émis aux termes de la PC sont assujettis aux politiques de sécurité de l'organisation; e) assurer la gestion de la configuration des environnements clients afin de minimiser les vulnérabilités; f) mettre en œuvre une politique de mots de passe selon laquelle, au minimum, (i) les mots de passe système par défaut choisis par le fournisseur sont changés immédiatement; (ii) les mots de passe choisis par le fournisseur ne sont pas utilisés; (iii) les postes de travail des clients, dans la mesure du possible, comportent des comptes utilisateurs protégés par mots de passe; (iv) les mots de passe, lorsque c'est possible, comportent au moins huit caractères, avec une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.

Déclarations et garanties du gestionnaire de référentiels

Lorsque l'AC exploite un référentiel ou qu'elle agit à titre de gestionnaire de référentiels, elle doit :

1. publier les certificats et les LCR;
2. faire connaître aux abonnés l'adresse des serveurs de LCR ou OCSP;
3. publier l'état des certificats dans des listes de certificats révoqués ou des serveurs OCSP, ou rendre cette information disponible dans les délais spécifiés dans les présentes politiques de certification;

4. configurer les contrôles d'accès du système d'exploitation et des référentiels de façon que seul le personnel autorisé de l'AC puisse écrire dans la version en ligne de la PC ou la modifier.

Lorsque l'AC n'exploite pas son propre référentiel, elle doit s'assurer, par des moyens contractuels ou autres, que le gestionnaire de référentiels satisfait aux exigences ci-dessus.

L'AC doit imposer des contrôles d'accès aux référentiels en ce qui concerne les certificats, les LCR ou la vérification en ligne de l'état des certificats.

Déclarations et garanties du propriétaire responsable d'application (PRA)

L'AC doit délivrer des certificats à l'égard des applications pour lesquelles le PRA a certifié à l'AC que l'application concernée satisfait à toutes les exigences des lois et des politiques pertinentes du Canada.

L'AC doit délivrer des certificats à l'égard des programmes pour lesquels le PRA a certifié à l'AC que des mesures appropriées ont été prises pour s'assurer que :

1. l'intégrité de l'application du programme est maintenue pendant toute sa durée de vie;
2. le logiciel du programme a été développé au moyen d'une méthode de conception structurée;
3. des mécanismes de sécurité intégrés sont mis en œuvre dans les applications;
4. les applications du programme :
   (a) satisfont aux exigences pertinentes du gouvernement du Canada en matière de protection des renseignements personnels;
   (b) ont été certifiées et accréditées conformément aux exigences de sécurité du gouvernement;
   (c) indiquent aux utilisateurs les vulnérabilités du point de vue de la sécurité et les correctifs;
   (d) indiquent explicitement quand une opération de signature numérique doit être effectuée;
   (e) effectuent une vérification de l'état des certificats tel que stipulé dans les sections 4.9.6 et 4.9.10.
5. une évaluation des menaces et des risques (EMR) conforme à la politique du gouvernement sur la sécurité a été effectuée;
6. une évaluation des facteurs relatifs à la vie privée (EFVP) conforme à la politique d'évaluation des facteurs relatifs à la vie privée a été effectuée, lorsque c'est nécessaire;
7. le PRA a évalué et pris en compte les problèmes de responsabilité potentiels découlant de la prestation de ce service en ligne et l'opportunité d'établir des limitations quant à la responsabilité, et il a pris des mesures pour s'assurer que les utilisateurs du service recevront un avis de ces limitations.

9.7 Stipulations d'exonération de garantie

Le gouvernement du Canada, ses employés, fonctionnaires ou agents n'offrent aucune représentation, garantie ou condition, explicite ou implicite, autres que celles qui sont expressément énoncées dans les présentes politiques de certification ou dans tout autre document autorisé à cette fin par le gouvernement du Canada.

Aucun partenariat, entreprise conjointe, fiducie, agence ou relation fiduciaire n'est établi ou présumé établi entre le gouvernement du Canada et les personnes, organisations ou toute autre partie qui utilisent les certificats émis par l'AC ou par une AC cocertifiée avec cette dernière.

9.8 Limitations de la responsabilité

Le gouvernement du Canada décline toute responsabilité que ce soit découlant de tout délit, contrat ou toute autre forme de réclamation, associée à l'utilisation, la délivrance, l'octroi sous licence ou l'emploi avec confiance des certificats émis en vertu des présentes politiques de certification, ou des paires de clés publiques/privées connexes, pour toute utilisation autre que celles qui sont prévues dans les présentes politiques de certification et tout autre accord ou entente écrite.

Le gouvernement du Canada décline toute responsabilité que ce soit découlant de tout délit, contrat ou toute autre forme de réclamation, associée à l'exportation ou à l'importation des produits cryptographiques par des personnes ou des organisations, en regard des programmes.

Le gouvernement du Canada décline toute responsabilité que ce soit découlant de toute action ou inaction de la part d'une organisation désignée, de toute nature, découlant de tout délit, contrat ou toute autre forme de réclamation, associée à l'utilisation, la délivrance, l'octroi sous licence ou l'emploi avec confiance de certificats, si une organisation désignée demande l'émission de certificats à des abonnés.

NIVEAU D'ASSURANCE	EXIGENCES
Assurance rudimentaire	L'Administration décline toute responsabilité de quelque nature que ce soit relativement aux attributions, aux dommages ou à toute autre réclamation ou obligation de quelque nature que ce soit découlant d'un délit, d'un contrat ou de toute autre raison en ce qui a trait à tout service associé à la délivrance, à l'emploi ou à la fiabilité d'un certificat de niveau rudimentaire de l'ICP du GC ou de la paire de clés privées/publiques associée. Les ministères peuvent établir leurs propres limites de responsabilité sur la base d'évaluations individuelles des menaces et des risques.
Assurance de base	L'Administration décline toute responsabilité de quelque nature que ce soit relativement aux attributions, aux dommages ou à toute autre réclamation ou obligation de quelque nature que ce soit découlant d'un délit, d'un contrat ou de toute autre raison en ce qui a trait à tout service associé à la délivrance, à l'emploi ou à la fiabilité d'un certificat d'assurance de niveau de base de l'ICP du GC ou de sa paire de clés privées/publiques associée, au-delà de **5 000 $** par montant adjugé, jugement ou règlement. Cette limite ne s'applique pas aux organisations désignées ou aux personnes responsables désignées qui peuvent accomplir des tâches d'AE. Les ministères peuvent établir leurs propres limites de responsabilité au-dessus du niveau recommandé sur la base d'évaluations individuelles des menaces et des risques.
Assurance moyenne	L'Administration décline toute responsabilité de quelque nature que ce soit relativement aux attributions, aux dommages ou à toute autre réclamation ou obligation de quelque nature que ce soit découlant d'un délit, d'un contrat ou de toute autre raison en ce qui a trait à tout service associé à la délivrance, à l'emploi ou à la fiabilité d'un certificat d'assurance de niveau de base de l'ICP du GC ou de sa paire de clés privées/publiques associée, au-delà de **50 000 $** par montant adjugé, jugement ou règlement. Cette limite ne s'applique pas aux organisations désignées ou aux personnes responsables désignées qui peuvent accomplir des tâches d'AE. Les ministères peuvent établir leurs propres limites de responsabilité

NIVEAU D'ASSURANCE	EXIGENCES
	au-dessus du niveau recommandé sur la base d'évaluations individuelles des menaces et des risques.
Assurance élevée	L'Administration décline toute responsabilité de quelque nature que ce soit relativement aux attributions, aux dommages ou à toute autre réclamation ou obligation de quelque nature que ce soit découlant d'un délit, d'un contrat ou de toute autre raison en ce qui a trait à tout service associé à la délivrance, à l'emploi ou à la fiabilité d'un certificat d'assurance de niveau de base de l'ICP du GC ou de sa paire de clés privées/publiques associée, au-delà de **100 000 $** par montant adjugé, jugement ou règlement. Cette limite ne s'applique pas aux organisations désignées ou aux personnes responsables désignées qui peuvent accomplir des tâches d'AE. Les ministères peuvent établir leurs propres limites de responsabilité au-dessus du niveau recommandé sur la base d'évaluations individuelles des menaces et des risques.

La maintenance des systèmes ou des facteurs qui échappent au contrôle de l'AC peuvent influer sur la disponibilité des services offerts par l'AC. Le gouvernement du Canada décline toute responsabilité de quelque nature que ce soit à l'égard des facteurs qui échappent à son contrôle, y compris la disponibilité ou le bon fonctionnement de l'Internet, des systèmes de télécommunication ou des autres systèmes d'infrastructure. Toute utilisation du terme « assurance » dans le présent document ne constitue nullement une représentation de garantie quant à la disponibilité de ces services.

L'AC décline toute responsabilité de quelque nature que ce soit à l'égard des applications qui utilisent les certificats qui sont émis par elle. En ce qui concerne l'utilisation des applications employées par un programme, les abonnés sont priés de consulter les ministères ou les organismes qui utilisent des certificats émis en vertu des présentes PC afin de déterminer s'ils ont établi des limites quant à leur responsabilité. Rien dans les présentes politiques de certification ne crée, n'altère ou n'abroge toute autre obligation ou responsabilité qui peut avoir été imposée ou assumée par un ministère ou un organisme qui emploie les services fournis par l'AC pour ses programmes respectifs. Il incombe au GOP concerné d'établir les limites de responsabilité du gouvernement du Canada à l'égard d'un programme.

Les droits, privilèges ou obligations, y compris les limitations de responsabilité, d'une partie utilisatrice qui est un abonné d'une autre AC peuvent faire l'objet d'une entente entre cet abonné et cette autre AC.

Les exonérations et limitations de responsabilité prévues dans les présentes PC sont assujetties à toute entente ou tout accord qui peut avoir été conclu par l'Administration et qui en dispose autrement.

9.9 Indemnités

Aucune exigence n'est stipulée.

9.10 Période et cessation des activités

9.10.1 Période

Aucune exigence n'est stipulée.

9.10.2 Cessation des activités

Les dispositions qui concernent la cessation des activités de l'AC sont stipulées dans la section 5.8 (Cessation des activités de l'AC).

9.10.3 Effet de la cessation des activités et survie

Aucune exigence n'est stipulée.

9.11 Avis individuels et communications avec les participants

Aucune exigence n'est stipulée.

9.12 Modifications

9.12.1 Procédure de modification

L'AGP de l'ICP du GC peut modifier les présentes politiques de certification, en tout ou en partie, en tout temps et à sa discrétion. Les ministères peuvent adopter ces politiques de certification à leurs propres fins. Avant de modifier les présentes politiques de certification, l'AGP de l'ICP du GC doit faire parvenir un avis de changement par écrit au Pont de l'ICP fédérale canadienne (PIFC) ainsi qu'à toutes les AC pour lesquelles il existe une certification croisée directe avec le PIFC, une période pour les commentaires pouvant être spécifiée dans cet avis.

9.12.2 Mécanisme de notification et période

L'AC doit :

1. fournir aux abonnés et aux parties utilisatrices l'URL d'un site Web;
2. publier sa PC, signée numériquement par un représentant autorisé de l'AC, sur le site Web évoqué ci-dessus;
3. informer, ou demander au Ministère d'informer, les abonnés et les parties utilisatrices de tout changement apporté concernant leurs droits, privilèges et obligations concernant les certificats;
4. fournir aux parties intéressées, à sa discrétion et aux termes et conditions qu'elle juge appropriés, tout ou partie de l'EPC, aux fins d'audit, d'inspection, d'accréditation ou de certification croisée.

9.12.3 Circonstances dans lesquelles l'OID doit être changé

Aucune exigence n'est stipulée.

9.13 Dispositions concernant le règlement des différends

Tout différend associé à la gestion des clés et des certificats entre le gouvernement du Canada et une organisation ou une personne à l'extérieur du gouvernement du Canada doit être résolu dans le cadre d'un mécanisme approprié de règlement des différends. Dans la mesure du possible, on recourra à la négociation pour régler les différends. Si un différend ne peut pas être réglé par la négociation, on doit faire appel à un médiateur indépendant, acceptable pour les parties en cause. Lorsque le différend ne peut pas être réglé par le médiateur, on doit recourir à l'arbitrage, conformément à la *Loi sur l'arbitrage commercial*.

Dans la mesure du possible, on doit recourir à la négociation pour régler les différends entre ministères portant sur la gestion des clés et des certificats. Lorsque le différend ne peut pas être réglé par la négociation, il doit l'être en ayant recours aux dispositions de résolution des conflits contenues dans le Protocole de certification croisée.

Un différend concernant la gestion des clés et des certificats au sein d'un ministère doit être résolu par l'autorité appropriée du ministère, en collaboration avec l'AC émettrice.

L'AC doit s'assurer que des mécanismes appropriés de règlement des différends sont inclus dans tout accord ou entente qu'elle conclut, ou dans toutes les modalités d'utilisation qu'elle établit.

9.14 Lois applicables

Les lois du Canada ainsi que les lois applicables des provinces et des territoires, à l'exclusion de leurs principes concernant les confilts de droit, régissent l'applicabilité, l'élaboration, l'interprétation et la validité des présentes politiques de certification.

Toute entente conclue par l'AC doit être régie par les lois du Canada ainsi que les lois applicables des provinces et des territoires, à l'exclusion de leurs principes concernant les conflits de droit, en ce qui concerne l'applicabilité, l'élaboration, l'interprétation et la validité des présentes politiques de certification.

9.15 Conformité aux lois applicables

Conformité à la législation sur la protection des renseignements personnels selon les exigences de la section 9.4 (Protection des renseignements personnels).

Conformité à la législation sur l'archivage selon les exigences de la section 9.16 (Archivage des documents).

9.16 Dispositions diverses

9.16.1 Accord intégral

Aucune exigence n'est stipulée.

9.16.2 Attribution

Aucune exigence n'est stipulée.

9.16.3 Divisibilité

S'il est déterminé qu'une partie de la présente PC est incorrecte ou invalide, le reste de la PC demeure en vigueur et valide.

9.16.4 Application (honoraires d'avocats et renonciation de droits)

Aucune exigence n'est stipulée.

9.16.5 Cas de force majeure

Aucune exigence n'est stipulée.

9.17 Autres dispositions

Aucune exigence n'est stipulée.

ANNEXE A – RFC3647

Conformité Mapping Sommaire

La v3.8 du document a été réorganisée afin de la rendre conforme à la norme établie par le document RFC3647. Cette opération a été effectuée en trois étapes, comme suit :

Étape 1 : Les correspondances exactes entre le texte / les sections de la v3.8 existante et l'aperçu du document RFC3647 sont indiquées dans le tableau ci-après :

v3.8 de la PC du GC	RFC3647
1. Introduction	1. INTRODUCTION
1.1 Aperçu	1.1 Aperçu
1.2 Identification des politiques	1.2 Nom et identification du document
1.3 Participants à l'ICP	1.3 Participants à l'ICP
1.3.1 Autorité de certification	1.3.1 Autorités de certification
1.3.2 Autorités d'enregistrement	1.3.2 Autorités d'enregistrement
1.3.3 Détenteurs de certificats	1.3.3 Abonnés
1.3.4 Abonnés	1.3.3 Abonnés
1.3.4 Abonnés	4.1.1 Qui peut présenter une demande de certificat
1.3.5 Organisations désignées	1.3.3 Abonnés
1.3.6 Parties utilisatrices	1.3.4 Parties utilisatrices
1.3.7 Autres participants	1.3.5 Autres participants
1.3.7 Autres participants	1.5.3 Personne qui détermine l'adéquation de l'EPC à l'égard de la politique
1.3.7 Autres participants	2.1 Référentiels
1.4 Utilisation des certificats	1.4 Utilisation des certificats
1.4.1 Utilisations appropriées des certificats	1.4.1 Utilisations appropriées des certificats
1.4.2 Utilisations interdites des certificats	1.4.2 Utilisations interdites des certificats
1.5 Administration des politiques	1.5 Administration des politiques
1.5.1 Organisation responsable des présentes politiques de certification	1.5.1 Organisation qui administre le document
1.5.2 Coordonnées	1.5.2 Personne contact
1.5.3 Avis et publication	2.2 Publication des informations de certification
1.5.3 Avis et publication	9.12.2 Période et mécanisme de notification
1.5.4 Modification des politiques de certification	9.12 Modifications
1.5.5 Approbation de l'Énoncé des pratiques de certification	1.5.4 Procédures d'approbation de l'EPC
1.6 Définitions et sigles	1.6 Définitions et sigles
1.6.1 Définitions générales	1.6 Définitions et sigles
1.6.2 Sigles	1.6 Définitions et sigles
2. Dispositions générales, légales et opérationnelles	9. AUTRES QUESTIONS ADMINISTRATIVES ET JURIDIQUES
2.1.7 Déclarations et garanties du PRA	5.2.4 Rôles nécessitant la séparation des fonctions
2.1 Déclarations et garanties	9.6 Déclarations et garanties
2.1.1 Déclarations et garanties de l'AC	4.2.3 Délai de traitement des demandes de certificat
2.1.1 Déclarations et garanties de l'AC	4.3.2 Notification à l'abonné par l'AC de la délivrance du certificat
2.1.1 Déclarations et garanties de l'AC	4.4.2 Publication du certificat par l'AC
2.1.1 Déclarations et garanties de l'AC	4.7.4 Notification à l'abonné de la délivrance d'un nouveau certificat
2.1.1 Déclarations et garanties de l'AC	4.10 Services d'état des certificats
2.1.1 Déclarations et garanties de l'AC	9.6.1 Déclarations et garanties de l'AC
2.1.2 Déclarations et garanties de l'AE	9.6.2 Déclarations et garanties de l'AE
2.1.3 Déclarations et garanties de l'abonné ou du détenteur de certificat	9.6.3 Déclarations et garanties de l'abonné
2.1.3 Déclarations et garanties de l'abonné	4.9.4 Période de grâce de la demande de révocation
2.1.4 Déclarations et garanties d'une organisation désignée	9.6.5 Déclarations et garanties des autres participants
2.1.5 Déclarations et garanties des parties utilisatrices	9.6.4 Déclarations et garanties des parties utilisatrices
2.1.6 Déclarations et garanties du gestionnaire de dépôt	2.2 Publication des informations de certification
2.1.6 Déclarations et garanties du gestionnaire de dépôt	2.4 Contrôles d'accès aux référentiels
2.1.6 Déclarations et garanties du gestionnaire de dépôt	9.6.5 Déclarations et garanties des autres participants
2.1.7 Déclarations et garanties du propriétaire responsable d'application	3.2.6 Critères d'interopérabilité
2.1.7 Déclarations et garanties du propriétaire responsable d'application	9.6.5 Déclarations et garanties des autres participants
2.2 Stipulations d'exonération de garanties	9.7 Avertissements concernant les garanties
2.3 Limitations de la responsabilité	9.8 Limitations de la responsabilité
2.3.1 Responsabilité financière	9.8 Limitations de la responsabilité
2.4.1 Cocertification	3.2.6 Critères d'interopérabilité
2.4.2 Reconnaissance des autres AC	3.2.6 Critères d'interopérabilité
2.4.3 Reconnaissance des certificats importés	3.2.6 Critères d'interopérabilité
2.5 Respect de l'information privée et protection des données	9.4 Confidentialité des informations personnelles
2.5 Respect de l'information privée et protection des données	9.4.5 Avis et consentement d'utilisation des informations privées
2.5.1 Sensibilité des types d'information privée	9.3 Confidentialité des informations commerciales
2.5.1 Sensibilité des types d'information privée	9.3.3 Responsabilité à l'égard de la protection des informations confidentielles
2.5.1 Sensibilité des types d'information privée	9.4.1 Plan de protection de la vie privée
2.5.1 Sensibilité des types d'information privée	9.4.2 Informations considérées privées
2.5.1 Sensibilité des types d'information privée	9.4.3 Informations non considérées privées
2.5.1 Sensibilité des types d'information privée	9.4.4 Responsabilité à l'égard de la protection des informations privées
2.5.2 Collecte permise d'information privée	9.4.2 Informations considérées privées

v3.8 de la PC du GC	RFC3647
2.5.3 Utilisation permise de l'information privée	9.4.5 Avis et consentement d'utilisation des informations privées
2.5.4 Distribution permise des renseignements personnels	9.4.7 Autres cas de divulgation de l'information
2.5.5 Possibilité pour une personne de corriger les renseignements personnels la concernant	9.4.2 Informations considérées privées
2.5.6 Divulgation d'information privée aux forces policières	9.4.6 Divulgation dans le cadre de procédures judiciaires ou administratives
2.5.7 Divulgation d'information privée en cas de procédures judiciaires	9.4.6 Divulgation dans le cadre de procédures judiciaires ou administratives
2.6 Responsabilité financière	9.2 Responsabilité financière
2.7.1 Lois applicables	9.14 Lois applicables
2.7.2 Procédure de règlement des différends	9.13 Dispositions concernant le règlement des différends
2.7.3 Divisibilité des dispositions	9.16.3 Divisibilité
2.8 Frais	9.1.1 Redevances pour la délivrance ou le renouvellement d'un certificat
2.9 Droits de propriété intellectuelle	9.5 Droits de propriété intellectuelle
3. Identification et authentification	3. IDENTIFICATION ET AUTHENTIFICATION (11)
3.1 Affectation des noms	3.1 Noms
3.1.1 Types de noms	3.1.1 Types de noms
3.1.2 Utilisation de noms intelligibles	3.1.2 Nécessité de l'utilisation de noms explicites
3.1.3 Anonymat des abonnés et des détenteurs de certificat	3.1.3 Anonymat ou pseudo-anomymat des abonnés
3.1.4 Règles d'interprétation des diverses formes de noms	3.1.4 Règles d'interprétation des diverses formes de noms
3.1.5 Unicité des noms	3.1.5 Unicité des noms
3.1.6 Reconnaissance, authentification et rôle des marques de commerce	3.1.6 Reconnaissance, authentification et rôle des marques de commerce
3.2 Validation initiale de l'identité	3.2 Validation initiale de l'identité
3.2.1 Méthode de preuve de possession d'une clé privée	3.2.1 Méthode de preuve de possession d'une clé privée
3.2.2 Authentification de l'identité d'une organisation	3.2.2 Authentification de l'identité d'une organisation
3.2.3 Authentification de l'identité d'une personne	3.2.3 Authentification de l'identité d'une personne

v3.8 de la PC du GC	RFC3647
3.2.3 Authentification de l'identité d'une personne	3.2.5 Validation de l'autorité
3.2.3 Authentification de l'identité d'une personne	1.3.3 Abonnés
3.3 Identification et authentification des demandes de renouvellement de clé	3.3 Identification et authentification des demandes de renouvellement de clé
3.3.1 Identification et authentification pour le renouvellement de routine des clés	4.7.2 Qui peut demander la certification d'une nouvelle clé publique
3.3.1 Identification et authentification pour le renouvellement de routine des clés	4.7.3 Traitement des demandes de renouvellement de clé
3.3.1 Identification et authentification pour le renouvellement de routine des clés	3.3.1 Identification et authentification pour le renouvellement courant des clés
3.3.2 Identification et authentification d'une demande de renouvellement de clés après leur révocation	3.3.2 Identification et authentification pour le renouvellement des clés après leur révocation
3.4 Identification et authentification des demandes de révocation	3.4 Identification et authentification des demandes de révocation
4. Exigences opérationnelles du cycle de vie des certificats	4. EXIGENCES OPÉRATIONNELLES DU CYCLE DE VIE DES CERTIFICATS (11)
4.1 Demande de certificat	4.1.1 Qui peut présenter une demande de certificat
4.1 Demande de certificat	4.1 Demande de certificat
4.1 Demande de certificat	4.1.1 Qui peut présenter une demande de certificat
4.1 Demande de certificat	4.2 Traitement des demandes de certificat
4.1 Demande de certificat	4.2.1 Fonctions d'identification et d'authentification
4.1 Demande de certificat	4.2.2 Approbation ou rejet des demandes de certificat
4.1 Demande de certificat	4.5 Utilisation des paires de clés et des certificats
4.1 Demande de certificat	4.5.1 Utilisation du certificat et de la clé privée de l'abonné
4.2 Émission des certificats	4.3 Délivrance des certificats

v3.8 de la PC du GC	RFC3647
4.3 Acceptation des certificats	4.4 Acceptation des certificats
4.3 Acceptation des certificats	4.4.1 Conduite constituant l'acceptation d'un certificat
4.4 Révocation d'un certificat	5.7.3 Procédures lors de la compromission de la clé privée d'une entité
4.4 Révocation ou suspension d'un certificat	4.9 Révocation et suspension d'un certificat
4.4.1 Motifs de révocation	4.9.1 Motifs de révocation
4.4.10 Exigences relatives à la vérification des LCR	4.9.6 Exigences relatives à la vérification de la révocation pour les parties utilisatrices
4.4.11 Vérification en ligne de l'état et de la révocation des certificats	4.9.9 Possibilité de la vérification en ligne de l'état et de la révocation des certificats
4.4.12 Exigences relatives à la vérification en ligne des certificats révoqués	4.9.10 Exigences relatives à la vérification en ligne des certificats révoqués
4.4.13 Autres formes de publications des certificats révoqués	4.9.11 Autres formes de publication des certificats révoqués
4.4.14 Exigences de vérification pour les autres modes de publication des certificats révoqués	4.9.11 Autres formes de publication des certificats révoqués
4.4.2 Qui peut demander une révocation	4.9.2 Qui peut demander la révocation
4.4.3 Procédure de demande de révocation	4.9.3 Procédure de demande de révocation
4.4.4 Période de grâce pour les demandes de révocation	4.9.5 Délai à l'intérieur duquel l'AC doit traiter la demande de révocation
4.4.5 Circonstances de la suspension	4.9.13 Circonstances de la suspension
4.4.6 Qui peut demander une suspension	4.9.14 Qui peut demander la suspension
4.4.7 Procédure de demande de suspension	4.9.15 Procédure de demande de suspension
4.4.8 Limites de période de suspension	4.9.16 Limites de la période de suspension
4.4.9 Fréquence d'émission des LCR	4.9.7 Fréquence de publication des LCR (le cas échéant)
5. Contrôles – Installation, gestion et opération	5. INSTALLATIONS, GESTION ET CONTRÔLES OPÉRATIONNELS (11)
5.1 Contrôles physiques	5.1 Contrôles physiques

v3.8 de la PC du GC	RFC3647
5.1.1 Emplacement et construction des installations	5.1.1 Emplacement et construction des installations
5.1.2 Accès physique	5.1.2 Accès physique
5.1.3 Alimentation électrique et climatisation	5.1.3 Alimentation électrique et climatisation
5.1.4 Exposition à l'eau	5.1.4 Exposition à l'eau
5.1.5 Prévention et protection contre les incendies	5.1.5 Prévention et protection contre les incendies
5.1.6 Stockage des supports	5.1.6 Stockage des supports
5.1.7 Mise au rebut des déchets	5.1.7 Élimination des déchets
5.1.8 Sauvegarde hors site	5.1.8 Sauvegarde hors site
5.2 Contrôles des procédures	5.2 Contrôles procéduraux
5.2.1 Rôles de confiance de l'AC	5.2.1 Rôles de confiance
5.2.2 Rôles de confiance de l'AE	5.2.1 Rôles de confiance
5.2.3 Nombre de personnes requises par tâche	5.2.2 Nombre de personnes requises par tâche
5.2.4 Identification et authentification de chaque rôle	5.2.3 Identification et authentification pour chaque rôle
5.3 Contrôles du personnel	5.3 Contrôles du personnel
5.3.1 Compétences, expérience et exigences d'attestation de sécurité	5.3.1 Qualifications, expérience et habilitation requises
5.3.2 Procédures de vérification des antécédents	5.3.2 Procédures de vérification des antécédents
5.3.3 Exigences relatives à la formation	5.3.3 Exigences relatives à la formation
5.3.4 Fréquence et exigences de recyclage	5.3.4 Fréquence et exigences de recyclage
5.3.5 Fréquence et séquence de rotation des emplois	5.3.5 Fréquence et séquence de rotation des emplois
5.3.6 Sanctions pour les actions non autorisées	5.3.6 Sanctions pour les actions non autorisées
5.3.7 Exigences pour les entrepreneurs indépendants	5.3.7 Exigences pour les entrepreneurs indépendants
5.3.8 Documentation fournie au personnel	5.3.8 Documentation fournie au personnel
5.4 Procédure de journalisation de vérification	5.4 Procédures de journalisation des événements
5.4.1 Types d'événements consignés	5.4.1 Types d'événements journalisés
5.4.2 Fréquence de traitement des journaux de vérification	5.4.2 Fréquence de traitement des journaux
5.4.3 Période de rétention des journaux de vérification	5.4.3 Période de rétention des journaux d'audit

v3.8 de la PC du GC	RFC3647
5.4.4 Protection des journaux de vérification	5.4.4 Protection des journaux d'audit
5.4.5 Procédures de sauvegarde des journaux de vérification	5.4.5 Procédures de sauvegarde des journaux d'audit
5.4.6 Système de collecte des vérifications	5.4.6 Système de collecte des données d'audit (internes ou externes)
5.4.7 Envoi d'un avis au sujet ayant causé un événement	5.4.7 Envoi d'un avis au sujet ayant causé un événement
5.4.8 Évaluation des vulnérabilités	5.4.8 Évaluation des vulnérabilités
5.5 Archivage des enregistrements	5.5 Archivage des documents
5.5 Archivage des enregistrements	5.5.1 Types de documents archivés
5.5 Archivage des enregistrements	5.5.2 Période de rétention des documents archivés
5.5 Archivage des enregistrements	5.5.3 Protection des documents archivés
5.5 Archivage des enregistrements	5.5.4 Procédures de sauvegarde des documents archivés
5.5 Archivage des enregistrements	5.5.7 Procédures d'obtention et de vérification des informations archivées
5.6 Renouvellement des clés	5.6 Renouvellement des clés
5.7 Récupération en cas de compromission et de sinistre	5.7 Compromission et reprise après sinistre
5.7.1 Corruption des ressources informatiques, des logiciels et/ou des données	5.7.2 Corruption des ressources informatiques, des logiciels et/ou des données
5.7.2 Révocation du certificat public de l'AC	5.7.1 Procédures de traitement des incidents et des compromissions
5.7.3 Compromission de la clé de l'AC	5.7.1 Procédures de traitement des incidents et des compromissions
5.7.4 Capacité de poursuivre les activités après un sinistre	5.7.4 Capacité de poursuivre les activités après un sinistre
5.8 Cessation ou modification des activités de l'AC	5.8 Cessation des activités de l'AC ou de l'AE
6. Contrôles techniques de sécurité	6. CONTRÔLES DE SÉCURITÉ TECHNIQUES (11)
6.1 Production et installation des paires de clés	6.1 Génération et installation des paires de clés

v3.8 de la PC du GC	RFC3647
6.1.1 Production des paires de clés	6.1.1 Génération des paires de clés
6.1.2 Livraison des clés privées à un abonné/détenteur de certificat	6.1.2 Fourniture de la clé privée à l'abonné
6.1.3 Livraison des clés publiques à l'émetteur de certificat	6.1.3 Fourniture de la clé publique à l'émetteur du certificat
6.1.4 Livraison des clés publiques de l'AC aux abonnés et aux détenteurs de certificat	6.1.4 Fourniture de la clé publique de l'AC aux parties utilisatrices
6.1.5 Tailles des clés	6.1.5 Taille des clés
6.1.6 Production des paramètres des clés publiques et vérification de la qualité	6.1.6 Génération des paramètres de la clé publique et contrôle de la qualité
6.1.7 Utilisation des clés (champ Key Usage selon x509ver.3)	6.1.7 Utilisation des clés (champ Key Usage selon x509ver.3)
6.2 Protection des clés privées et contrôles techniques des modules cryptographiques	6.2 Protection des clés privées et contrôles techniques des modules cryptographiques
6.2.1 Normes et contrôles des modules cryptographiques	6.2.1 Normes et contrôles des modules cryptographiques
6.2.10 Méthode de destruction des clés privées	6.2.10 Méthode de destruction des clés privées
6.2.2 Contrôle multi-personne des clés privées	6.2.2 Contrôle multi-personne des clés privées (n sur m)
6.2.3 Entiercement des clés privées	4.12 Séquestre et récupération des clés
6.2.3 Entiercement des clés privées	4.12.1 Politique et pratiques de séquestre et de récupération des clés
6.2.3 Entiercement des clés privées	6.2.3 Séquestre des clés privées
6.2.4 Sauvegarde des clés privées	6.2.4 Sauvegarde des clés privées
6.2.5 Archivage des clés privées	6.2.5 Archivage des clés privées
6.2.6 Transfert des clés privées en direction ou en provenance d'un module cryptographique	6.2.6 Transfert des clés privées en direction ou en provenance d'un module cryptographique
6.2.7 Entreposage des clés privées dans un module cryptographique	6.2.7 Stockage de la clé privée dans un module cryptographique
6.2.8 Méthode d'activation des clés privées	6.2.8 Méthode d'activation de la clé privée
6.2.9 Méthode de désactivation des clés privées	6.2.9 Méthode de désactivation de la clé privée

v3.8 de la PC du GC	RFC3647
6.3 Autres aspects de la gestion des paires de clés	6.3 Autres aspects de la gestion des paires de clés
6.3.1 Archivage des clés publiques	6.3.1 Archivage de la clé publique
6.3.2 Périodes opérationnelles des certificats et périodes d'utilisation des paires de clés	6.3.2 Périodes opérationnelles des certificats et périodes d'utilisation des paires de clés
6.3.3 Entreposage, sauvegarde et récupération des clés de l'AC	6.2.4 Sauvegarde de la clé privée
6.3.4 Récupération des clés par l'abonné ou le détenteur de certificat	4.12.1 Politique et pratiques de séquestre et de récupération des clés
6.4 Données d'activation	6.4 Données d'activation
6.4.1 Production et installation des données d'activation	6.4.1 Génération et installation des données d'activation
6.4.2 Protection des données d'activation	6.4.2 Protection des données d'activation
6.4.3 Autres aspects des données d'activation	6.4.3 Autres aspects des données d'activation
6.5 Contrôles de sécurité informatique	6.5 Contrôles de sécurité informatique
6.5.1 Exigences techniques particulières de sécurité informatique	6.5.1 Exigences techniques particulières de la sécurité informatique
6.5.2 Évaluation de la sécurité informatique	6.5.2 Évaluation de la sécurité informatique
6.6 Contrôles techniques du cycle de vie	6.6 Contrôles techniques du cycle de vie
6.6.1 Contrôles du développement du système	6.6.1 Contrôles sur le développement du système
6.6.2 Contrôles de gestion de la sécurité	6.6.2 Contrôles de gestion de la sécurité
6.7 Contrôles de sécurité réseau	6.7 Contrôles de sécurité réseau
6.8 Horodatage	6.8 Horodatage
7. Profils des certificats et des LCR	7. PROFILS DES CERTIFICATS, DES LCR ET OCSP
7.1 Profil des certificats	7.1 Profil des certificats
7.1.1 Numéro de version	7.1.1 Numéro de version
7.1.2 Champs additionnels du certificat	7.1.2 Extensions du certificat
7.1.3 Identificateurs d'objets des algorithmes	7.1.3 Identificateurs d'objets des algorithmes
7.1.4 Forme des noms	7.1.4 Forme des noms
7.1.5 Contraintes relatives au nom	7.1.5 Contraintes relatives au nom
7.1.6 Identificateur d'objet d'une politique de certification	7.1.6 Identificateur d'objet d'une politique de certification
7.1.7 Utilisation de l'extension des contraintes de politique	7.1.7 Utilisation de l'extension des contraintes de politique
7.1.8 Syntaxe et sémantique des qualifiants des politiques	7.1.8 Syntaxe et sémantique des qualificateurs de politiques
7.1.9 Sémantique de traitement des extensions critiques des certificats	7.1.9 Sémantique de traitement des extensions critiques de politiques de certification
7.2 Profil des LCR	7.2 Profil des LCR
7.2.1 Numéro de version	7.2.1 Numéro de version
7.2.2 LCR et extensions des entrées des LCR	7.2.2 LCR et extensions des entrées des LCR
7.3 Profil OCSP	7.3 Profil OCSP
7.3.1 Numéro de version	7.3.1 Numéro de version
7.3.2 Extensions OCSP	7.3.2 Extensions OCSP
8. Inspection de conformité et autres évaluations	8. AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS
8.1 Fréquence ou circonstances des évaluations	8.1 Fréquence ou circonstances des évaluations
8.2 Identité et compétences de l'évaluateur	8.2 Identité et qualifications de l'évaluateur
8.3 Relations de l'évaluateur avec l'entité évaluée	8.3 Relations de l'évaluateur avec l'entité évaluée
8.4 Sujets couverts par l'évaluation	8.4 Sujets couverts par l'évaluation
8.5 Mesures prises suite au constat de lacunes	8.5 Mesures prises suite au constat de lacunes
8.6 Communication des résultats	8.6 Communication des résultats

Étape 2 : Rubriques de la PC ancienne sans rubrique correspondante dans le document RFC3647 et qui ont été retirées.

Rubriques dans la v3.8 de la PC du GC sans rubrique correspondante dans le document RFC3647
2.4 Cocertification et reconnaissance
2.10 Règlementation des produits cryptographiques
4.1.1 Demande d'un cocertificat

Une nouvelle rubrique a été créée (en dérogation au document RFC3647) pour une rubrique existante de la PC qui devait être conservée dans le document.

3.5 Identification et authentification des demandes de récupération	4.13 Sauvegarde et récupération des clés

Étape 3 : Pour les rubriques du document RFC3647 qui n'ont pas de section correspondante dans la PC, on a établi un renvoi à les parties pertinentes du document (et ainsi minimisé la redondance).

Rubriques dans le document RFC3647	Renvoi à d'autres parties dans la PC
4.1.2 Processus d'inscription et responsabilités	Renvoi à 1.3 (Participants à l'ICP) et 3.2 (Validation de l'identité)
4.5.2 Utilisation de la clé publique et du certificat d'une partie utilisatrice	Renvoi à la section 3.2.6 (Critères d'interopérabilité) et à la section 9.6.4 (Déclarations et garanties de la partie utilisatrice)
4.7.4 Notification à l'abonné de la délivrance d'un nouveau certificat	Renvoi à 4.3.2 (Notification à l'abonné par l'AC de la délivrance d'un certificat)
4.7.5 Conduite constituant l'acceptation d'un certificat renouvelé	4.4.1 Conduite constituant l'acceptation d'un certificat
4.7.6 Publication par l'AC du certificat renouvelé	Renvoi à 4.4.2 (Publication du certificat par l'AC)
4.7.7 Notification de la délivrance d'un certificat par l'AC à d'autres entités	Renvoi à 4.4.3 (Notification de la délivrance d'un certificat par l'AC à d'autres entités)
4.9.12 Exigences spéciales concernant la compromission d'une clé	Renvoi à 4.9.7 (Fréquence de publication de la LCR) et à 4.9.9 (Vérification en ligne de l'état et de la révocation)
4.10.1 Caractéristiques opérationnelles	Renvois à 7.2 (Profil de la LCR) et à 7.3 (Profil OCSP)
4.10.2 Disponibilité du service	Renvois à 4.9.7 (Fréquence de publication de la LCR) et à 4.9.9 (Vérification en ligne de l'état et de la révocation)
4.11 Fin de l'abonnement	Renvoi à 4.9.1 (Circonstances de la révocation)
5.2.4 Rôles nécessitant une séparation des fonctions	Renvoi à 5.2.1 (Rôles de confiance)
5.7.3 Procédures en cas de compromission de la clé privée d'une entité	Renvoi à 4.9 (Révocation ou suspension d'un certificat)

6.2.11 Évaluation du module cryptographique	Renvoi à 6.2.1 (Normes et contrôles des modules cryptographiques)
9.6.5 Déclarations et garanties des autres participants (PRA)	Renvoi à 3.2.6 (Critères d'interopérabilité)
9.10.2 Cessation des activités	Renvoi à 5.8 (Cessation des activités de l'AC ou de l'AE)
9.15 Conformité à la législation pertinente	Renvois à 9.4.1 (Plan de protection de la vie privée) et à 5.5 (Archivage des documents)