Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Ligne directrice sur la gestion de l'infrastructure à clé publique au gouvernement du Canada

Publié : le 07 janv. 2011

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

N° de catalogue BT22-170/2011F-PDF
ISBN : 978-0-660-09790-9

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Guideline on the Management of Public Key Infrastructure in the Government of Canada

Ligne directrice sur la gestion de l'infrastructure à clé publique au gouvernement du Canada

1.Contexte

Le 1er juillet 2009, la Politique de gestion de l'infrastructure à clé publique au gouvernement du Canada (Politique sur l'ICP) était abrogée. La présente Ligne directrice a pour but d'aider les ministères et les gestionnaires de programme à comprendre comment les responsabilités et les pratiques établies par la Politique sur l'ICP ont évolué conformément aux exigences de la Politique sur la sécurité du gouvernement (PSG).

La Ligne directrice décrit les pratiques recommandées pour la gouvernance et la gestion de l'Infrastructure à clé publique (ICP) au gouvernement du Canada (GC), avec les conseils opérationnels qui s'imposent. Elle ne renferme toutefois pas d'avis, de conseils ni d'exigences techniques quant à la mise en œuvre de la technologie à clé publique par les ministères et organismes du GC.

La Politique sur l'ICP a été établie afin de concrétiser la position du GC, qui veut faire de la technologie à clé publique son moyen de prédilection pour authentifier électroniquement l'identité des entités ou des individus, et de rehausser l'intégrité et la confidentialité des documents.

Dans le contexte de l'initiative de renouvellement de l'ensemble des politiques, la Politique sur l'ICP a été abrogée afin d'harmoniser les responsabilités et la reddition de comptes en ce qui concerne les opérations électroniques sécurisées aux termes de la PSG et des instruments connexes. Cela assurera une approche uniforme pour la sécurisation des activités électroniques de l'administration gouvernementale, en rendant possibles différentes options d'authentification électronique qui devraient permettre au GC d'obtenir les résultats escomptés en matière de sécurité et d'identité, tout en donnant aux ministères et aux organismes la marge de manœuvre nécessaire pour qu'ils puissent se servir des technologies les mieux adaptées à leurs propres exigences opérationnelles.

2. Gouvernance de l'ICP au Gouvernement de Canada

Alors que la Politique sur l'ICP favorisait l'utilisation des technologies à clé publique, la PSG et ses instruments connexes sont censés être technologiquement neutres. Pour obtenir les résultats auxquels le GC s'attend en matière de sécurité et pour faire en sorte que l'information, les biens, les services et les interactions soient protégés à cet égard, la PSG, la Directive sur la gestion de la sécurité ministérielle (DGSM) et la Directive sur la gestion de l'identité (DGI) précisent les exigences à l'échelle du GC applicables à l'établissement de procédés basés sur la gestion des risques grâce auxquels les ministères et les organismes pourront efficacement contrer leurs risques en matière de sécurité et d'identité.

Les normes et les lignes directrices qui étayent la PSG et ses directives servent à promouvoir les pratiques communes et/ou exemplaires dans tout le GC, sans toutefois chercher à prescrire la méthode, la solution, l'outil ou la technologie que les ministères et les organismes doivent employer pour atteindre les objectifs de contrôle de la sécurité. Il s'ensuit que ***les ministères et les organismes ont plus de latitude que jamais dans le choix des technologies répondant le mieux à leurs besoins; l'ICP est l'une des options qui s'offrent à eux***.

2.1 Lois et règlements applicables

La liste des lois fédérales applicables à la signature électronique et aux documents électroniques, présentée sous cette rubrique, n'est pas exhaustive. ***Les ministères et les organismes devraient consulter leurs services juridiques pour déterminer quelle loi s'applique à leurs fins particulières, s'il y a lieu.***

Cela dit, la partie 2 de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) établit un cadre décrivant des moyens électroniques dont on peut se servir plutôt que de papier pour créer des documents ou pour communiquer de l'information ou des opérations dans les cas où une loi ou un règlement prévoit l'utilisation du papier (p. ex., quand une loi fédérale fait état d'« originaux », de « déclarations sous serment », d'une « affirmation solennelle », de « déclarations attestant la véracité, l'exactitude ou l'intégralité », de documents portant un sceau et de la signature d'un témoin).

L'article 31.4 de la Loi sur la preuve au Canada (LPC) investit le gouverneur en conseil du pouvoir de prendre des règlements établissant des présomptions relatives à la preuve relativement aux documents électroniques portant une signature électronique sécurisée.

Le Règlement sur les signatures électroniques sécurisées (Règlement sur les SES) adopté en vertu de la LPRPDE et de la LPC, prescrit la technologie et le processus requis pour l'obtention des signatures électroniques sécurisées, et établit les présomptions relatives à la preuve applicables lorsqu'on utilise la technologie et le processus prescrits à l'égard des données contenues dans un document électronique.

La rubrique « Reconnaissance d'une AC » de cette ligne directrice contient d'autres renseignements sur les signatures électroniques sécurisées.

2.2 Politiques, directives et normes applicables

Cette rubrique précise et décrit les politiques, les directives et les normes applicables que les ministères et les organismes

devraient consulter lorsqu'ils doivent décider s'ils devraient mettre une ICP en place pour répondre à leurs besoins. Nous avons cité les extraits pertinents de ces documents pour qu'il soit plus facile de s'y reporter, mais le lecteur devrait consulter les originaux pour avoir le contexte intégral.

La PSG définit au sens large le besoin d'établir un sentiment de confiance dans les interactions avec les services et les programmes du gouvernement, sans toutefois prescrire les mécanismes qu'il faudrait employer à cette fin :

La sécurité commence par l'établissement d'un sentiment de confiance dans les interactions entre le gouvernement et la population et à l'intérieur du gouvernement[1].

L'annexe C de la DGSM stipule que les ministères ont la responsabilité de choisir des moyens de contrôle de la sécurité correspondant à leurs besoins :

Les ministères sont responsables de sélectionner, de mettre en œuvre, de surveiller et de maintenir des moyens durables de contrôle de la sécurité afin d'atteindre les objectifs en matière de contrôles de sécurité. Les mesures de contrôle de sécurité peuvent être de nature administrative, gestionnelle, opérationnelle, technique ou procédurale. Les contrôles de sécurité obligatoires et recommandés sont précisés dans les normes et lignes directrices qui appuient la Politique sur la sécurité au gouvernement. Les ministères peuvent prendre d'autres mesures de contrôle de sécurité et se fixer des objectifs de contrôle additionnels en se fondant sur les résultats des évaluations des risques[2].

La DGSM précise de façon plus détaillée les responsabilités applicables au choix des moyens de contrôle de la sécurité ainsi qu'à l'évaluation et à l'acceptation des niveaux de risque résiduel des programmes et des services. Elle précise que les praticiens ministériels en matière de sécurité sont responsables de :

sélectionner, mettre en œuvre et maintenir des contrôles de sécurité liés à leur champ de responsabilité afin d'assurer la réalisation des objectifs de contrôle[3].

En outre, la DGSM impose aux gestionnaires de tous les niveaux la responsabilité :

d'évaluer les risques en matière de sécurité, d'accepter officiellement les risques résiduels ou en recommander l'acceptation (ces risques sont définis dans le plan de sécurité ministérielle) et de réévaluer périodiquement les risques à la lumière des changements apportés aux programmes, aux activités ou aux services et de prendre des mesures correctives pour corriger les lacunes relevées[4].

La Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) explique cette responsabilité en ce qui concerne les gestionnaires chargés de l'exécution de programmes et de la prestation de services dans le domaine de la sécurité des technologies de l'information :

Au stade de la conception des programmes et services, les gestionnaires collaborent avec les spécialistes de la sécurité du ministère afin de gérer les risques liés à leurs programmes ou services. En s'appuyant sur les conseils et le support du coordonnateur de la sécurité des TI, les gestionnaires doivent déterminer les exigences de sécurité des TI pour leurs programmes et services et doivent les accréditer en acceptant le risque résiduel qui leur est associé[5].

La GSTI précise encore davantage les responsabilités de certification et d'accréditation des systèmes de TI au GC :

Pour les systèmes ou services communs, le dirigeant principal de l'information du gouvernement du Canada est le responsable de l'accréditation. Pour les systèmes ou services propres à un ministère, le gestionnaire de la prestation de programmes ou services est chargé de l'accréditation. Pour les systèmes ou services communs à deux organisations ou plus, le gestionnaire du programme ou du service est responsable de l'accréditation[6].

Ces responsabilités s'appliquent à la certification et à l'accréditation des systèmes d'ICP au GC. Il s'ensuit que le gestionnaire responsable de l'exécution du programme ou de la prestation du service devrait s'assurer (avec l'aide des spécialistes de la sécurité du ministère) que toutes les politiques, tous les processus ou toutes les technologies mis en place pour s'assurer que le système d'ICP sont adaptés aux besoins et capables d'y répondre quand ils prennent leur décision d'accréditer un système quelconque.

Auparavant, la gouvernance et la gestion de l'ICP au GC étaient expressément définies par les mécanismes que prescrivait la Politique sur l'ICP, mais l'ICP devrait désormais être gérée conformément aux exigences de la PSG et des directives ainsi que des normes connexes sur la sécurité du GC (plus particulièrement la GSTI). Par suite de l'abrogation de la Politique sur l'ICP, les ministères qui choisissent l'ICP comme moyen de contrôle de la sécurité devraient constater qu'ils disposent d'une plus grande marge de manœuvre pour gérer leur ICP.

3. Gestion de l'ICP au Gouvernement du Canada

3.1 Classes d'autorités de certification au gouvernement du Canada

Cette rubrique distingue les types d'autorité de certification (AC) qui peuvent être utiles aux ministères pour s'acquitter de leurs exigences en matière d'ICP.

3.1.1 AC commune

Au GC, une AC commune délivre des certificats de clé publique (CCP) au nom d'autres ministères ou d'utilisateurs externes. **L'AC des services communs de gestion des justificatifs internes (GJI)** administrée par TPSGC pour le compte du Secrétariat du Conseil du Trésor (SCT) est l'AC commune approuvée pour les ministères qui ont besoin de certificats d'ICP pour leurs systèmes internes gouvernementaux contenant de l'information jusqu'au niveau « Protégé B ». Les ministères devraient consulter la Politique sur les services communs et le Guide ministériel pour l'adoption des services obligatoires de la Voie protégée pour s'informer des utilisations obligatoires de ce service. L'AC des services communs de GJI a été reconnue par le président du Conseil du Trésor comme conforme au Règlement sur les SES.

TPSGC gère aussi le service d'**AC du gouvernement en direct (GED)** pour le compte du SCT, en délivrant des certificats aux utilisateurs de l'extérieur du gouvernement. L'AC du GED est approuvée pour des utilisations allant jusqu'au niveau d'information « Protégé B ».

Les ministères devraient communiquer avec leur représentant au service à la clientèle de TPSGC pour lui parler de leurs objectifs et pour savoir si ces AC communes peuvent les aider à répondre à leurs besoins. Lorsqu'un ministère a un besoin d'AC commune auquel l'AC de services communs de GJI ne peut pas répondre, il devrait communiquer le plus tôt possible avec le SCT afin de cerner ce besoin et de préciser pourquoi l'AC des services communs de GJI n'y répond pas. À partir de là, on trouvera un moyen d'aller de l'avant en définissant les rôles et les responsabilités en vue de la certification et de l'accréditation du système. On devrait pouvoir faire une certification réciproque (ou cocertification) avec une AC commune grâce à la Charnière fédérale canadienne de l'ICP quand elle s'y prête (voir 3.1.3 et 3.2, plus loin).

Les ministères ou les gestionnaires de programmes désireux d'établir une AC commune devraient :

- communiquer avec la Division de la gestion de la sécurité et de l'identité (DGSI) de la Direction du dirigeant principal de l'information (DDPI) du SCT pour préciser leurs besoins;
- faire en sorte qu'on élabore des plans de certification et d'accréditation et qu'on les envoie au SCT pour examen avant l'accréditation définitive.

3.1.2 AC ministérielle

Les ministères se servent de leur **AC ministérielle** pour répondre à un besoin interne lorsqu'ils ne sont pas tenus d'avoir recours à l'AC des services communs de GJI du GC (voir la rubrique qui précède sur l'**AC commune**) et que celle-ci ne peut pas répondre de façon satisfaisante aux besoins du ministère.

Pour son AC ministérielle, le ministère devrait s'assurer qu'on a bien géré les risques dans le système. Conformément à la GSTI, c'est le gestionnaire du ministère qui est chargé de l'exécution du programme ou de la prestation du service qui est responsable de l'accréditation du système. Les ministères disposent de la marge de manœuvre nécessaire pour déterminer les exigences de sécurité applicables à leurs AC ministérielles dans leur fourchette de tolérances des risques. Il est recommandé qu'ils se conforment aux pratiques exemplaires du secteur privé pour établir leurs exigences de sécurité et qu'ils harmonisent dans toute la mesure du possible leurs politiques et leurs pratiques de certification avec celles de la Charnière fédérale canadienne de l'ICP (voir 3.1.3, plus loin).

Les AC ministérielles peuvent être par exemple :

- des AC conçues pour délivrer des certificats de couche de sécurité pour le transport (CST) à des fins ministérielles internes seulement (autrement dit pas pour délivrer des certificats à d'autres ministères ou au public);
- des AC assorties d'exigences de confiance spécifiques telles qu'il est impossible d'avoir recours à une AC commune;
- des AC conçues pour délivrer des certificats internes de grandes assurances ou des certificats destinés à être utilisés dans un système fermé (p. ex., classifié).

Les ministères ou les gestionnaires de programmes qui établissent une AC ministérielle devraient :

- s'assurer que l'AC commune du GC ne peut pas satisfaire à leurs exigences, en en parlant avec le gestionnaire des relations avec la clientèle de l'OSPTI de TPSGC du ministère;
- demander une dérogation à la Politique sur les services communs pour l'AC;
- communiquer avec le Centre de la sécurité des télécommunications Canada (CSTC) pour obtenir des conseils sur les mesures de chiffrement et sur la gestion des clés, s'il y a lieu;
- s'assurer qu'on a établi des plans de certification et d'accréditation des systèmes et qu'on les a appliqués;
- s'assurer que l'AC a été accréditée conformément à leur norme ministérielle avant d'avoir été mise en œuvre.

3.1.3 AC charnière

Une AC charnière (ou charnière d'ICP) est une AC servant à établir une relation de confiance entre des systèmes d'ICP séparés distincts. La relation de confiance est établie grâce à un processus de certification réciproque entre différentes AC.

Au GC, la **Charnière fédérale canadienne de l'ICP** (CCFICP) est l'AC charnière approuvée. Elle est gérée par le CSTC pour le compte du SCT.

3.2 Certification réciproque

La certification réciproque est un processus dont les AC se servent pour établir une relation de confiance dans lequel une AC délivre un certificat à une autre AC. Les certifications réciproques peuvent aussi être combinées, les rôles des AC qui

délivrent la certification et qui la reçoivent ou qui s'en servent pouvant être inversés (ce qui revient à une certification réciproque mutuelle). Quand deux AC se certifient réciproquement, elles conviennent de se fier à leurs CCP et à leurs clés réciproques comme si elles avaient délivré les certificats elles-mêmes. Les ministères du GC qui sont tenus de certifier réciproquement leur AC avec une autre AC de l'extérieur de leur organisation devraient le faire en passant par la Charnière fédérale canadienne de l'ICP, ce qui nécessite des certifications réciproques entre les AC du GC et des AC de l'extérieur du GC.

Le président du Conseil du Trésor est investi par décret du pouvoir de conclure ou de résilier des ententes de certification réciproque ou de reconnaissance d'AC, incluant celles de l'extérieur du GC. Il a délégué ce pouvoir au dirigeant principal de l'information du gouvernement du Canada.

Aperçu du processus de certification réciproque :

- Le demandeur doit établir le besoin opérationnel d'une certification réciproque avec la CCFICP.
- Le demandeur soumet sa demande à la DDPI.
- Dans le cas d'une organisation de l'extérieur du GC, un ministère fédéral devra agir comme parrain.
- Les politiques de certification de l'AC qui fait la demande seront examinées pour en assurer l'harmonisation avec celles de la CCFICP.
- Un banc d'essais sera réalisé.
- Une entente officielle sera négociée et signée.
- L'AC qui fait la demande et la CCFICP échangeront les certificats.

Veuillez communiquer avec la Direction de la gestion de la sécurité et de l'identité de la DDPI, aux coordonnées indiquées sous la rubrique « Demandes de renseignements » de cette ligne directrice, si vous avez besoin de renseignements détaillés sur le processus de certification réciproque ou si vous voulez déterminer la nécessité d'une telle certification.

3.3 Reconnaissance d'une AC

3.3.1 Applicabilité

La reconnaissance d'une AC s'entend des exigences officielles auxquelles il faut satisfaire pour sécuriser une signature électronique conformément à la partie 2 de la LPRPDE. En vertu du Règlement sur les SES, le président du Conseil du Trésor peut reconnaître une entité ou un individu en tant qu'AC. Toutefois, avant de le faire, il doit être convaincu que l'individu ou l'entité a la capacité de délivrer des certificats de signature numérique sécurisée de façon fiable, conformément aux alinéas 48(2)*a*) à *d*) de la LPRPDE, qui disposent que :

- la signature électronique résultant de l'utilisation de la technologie ou du procédé est propre à l'utilisateur;
- l'utilisation de la technologie ou du procédé pour l'incorporation, l'adjonction ou l'association de la signature électronique de l'utilisateur au document électronique est sous le seul contrôle de ce dernier;
- la technologie ou le procédé permet d'identifier l'utilisateur;
- la signature électronique peut être liée au document électronique de façon à permettre de vérifier si le document a été modifié depuis que la signature électronique a été incorporée, jointe ou associée au document.

Les circonstances dans lesquelles les ministères devront faire reconnaître leur AC par le président du Conseil du Trésor sont très limitées. Avant de demander au SCT de reconnaître leur AC, ils devraient préciser leurs besoins à l'égard d'un programme ou d'une opération. ***Les ministères devraient également consulter leurs services juridiques pour déterminer si des facteurs font obstacle à ce qu'ils procèdent par des moyens électroniques et, s'il n'y a pas d'obstacle, si une signature électronique sécurisée aux termes de la LPRPDE et du Règlement sur les SES s'impose ou si une autre forme de signature électronique peut suffire***.

En général, une signature électronique sécurisée s'impose lorsqu'un ministère est tenu par sa loi de traiter des documents de papier signés, mais souhaite les remplacer par des documents électroniques. Une signature électronique sécurisée rend également possibles certaines présomptions relatives à la preuve établies par le Règlement sur les SES en vertu de la LPC. Pour pouvoir utiliser des signatures électroniques et bénéficier de ces présomptions, le ministère doit d'abord faire ajouter sa loi à la liste des annexes 2 ou 3 de la LPRPDE, puis se conformer au Règlement sur les SES, ce qui implique que le président du Conseil du Trésor doit reconnaître l'AC qui délivre les clés de signature. Le Règlement stipule que les AC reconnues comme étant capables de créer des signatures électroniques sécurisées doivent figurer sur le site Web du SCT. À l'heure actuelle, seules les AC du gouvernement fédéral qui ont fait l'objet d'une certification réciproque avec la Charnière fédérale canadienne de l'ICP sont admissibles à cette reconnaissance.

Lorsqu'un ministère a opté d'adhérer au régime susdécrit de la LPRPDE, il doit utiliser des signatures électroniques sécurisées pour les documents électroniques lorsque :

- un certificat ou autre document portant la signature d'un ministre ou d'un fonctionnaire public fait foi du contenu du document – LPRPDE, art. 36;
- la position du sceau d'une personne est exigée – LPRPDE, art. 39;
- un document original est exigé – LPRPDE, art. 42;
- une déclaration sous serment ou une affirmation solennelle est exigée – LPRPDE, art. 44;
- une déclaration attestant la véracité, l'exactitude ou l'intégralité d'une information fournie par le déclarant est exigée – LPRPDE, art. 45;
- la signature d'un témoin est exigée – LPRPDE, art. 46.

3.3.2 Aperçu du processus de reconnaissance

Il faut respecter les étapes suivantes de haut niveau afin d'accorder la reconnaissance d'une AC dans le contexte du Règlement sur les SES:

- Déterminer le besoin opérationnel de reconnaissance;
- Si cela n'est pas déjà fait, l'AC qui fait la demande doit obtenir une certification réciproque avec la CCFICP (processus décrit à la section 3.2);
- Le DPI du GC approuvera la demande de reconnaissance lorsqu'il sera convaincu que l'AC dispose des capacités nécessaires pour émettre de façon sûre et fiable des certificats de signature numérique (en tenant compte du contexte du Règlement sur les SES et de la LPRPDE);
- Dès l'approbation donnée, les détails concernant l'AC seront affichés dans le site Web du SCT;
- L'état de reconnaissance sera évalué chaque année. Aux fins du renouvellement de la reconnaissance, l'AC devra être encore en règle auprès de la CCFICP, en ce qui concerne la certification réciproque, et le responsable opérationnel de l'AC devra envoyer à la DDPI une lettre d'attestation de l'observation par l'AC de ses politiques de certification.

Veuillez communiquer avec la Direction de la gestion de la sécurité et de l'identité de la DDPI, aux coordonnées indiquées sous la rubrique « Demandes de renseignements » de cette ligne directrice, si vous avez besoin de renseignements additionnels sur la reconnaissance d'une AC.

4. Conseils opérationnels

Les ministères ou les gestionnaires de programmes qui choisissent de se servir de la technologie à clé publique comme moyen de protéger la confidentialité des renseignements ou d'authentifier électroniquement l'identité des individus et/ou des documents devraient :

4.1 Assurer l'harmonisation avec les politiques, les lois et les décrets du GC en:

- se servant de l'AC de services communs de GJI fournie par TPSGC afin de délivrer des certificats numériques d'assurance moyenne aux utilisateurs ou d'obtenir les dérogations appropriées afin d'établir leur propre autorité de certification ministérielle;
- utilisant la CCFICP gérée par le CSTC quand une certification réciproque est requise entre des AC communes et ministérielles ou lorsqu'une certification réciproque est requise avec des AC de l'extérieur du GC;
- s'assurant que l'utilisation et la gestion de l'ICP est compatible avec les buts du GC en matière de gestion de la sécurité et de l'identité établis par le Conseil du Trésor dans la PSG et dans ses instruments connexes.

4.2 Établir et maintenir des politiques de certification et des énoncés de pratiques de certification en:

- s'assurant que l'AC gère le CCP et les listes de certificats révoqués (LCR) qu'il délivre en mettant en œuvre une ou plusieurs politiques de certification et en publiant un énoncé de pratiques de certification sur le fonctionnement de cette autorité de certification;
- s'assurant que tous les individus ou toutes les entités qui agissent en son nom se conforment à ses politiques de certification et à ses énoncés de pratiques de certification;
- en harmonisant dans toute la mesure du possible ses politiques de certification et ses énoncés de pratiques de certification avec ceux de la CCFICP.

4.3 Noter et communiquer aux utilisateurs et aux parties qui s'y fient tous les droits et toutes les exigences, conditions et limites, en:

- s'assurant que les utilisateurs sont informés de leurs droits et de leurs obligations ainsi que des droits et des obligations de l'AC;
- élaborant, mettant en œuvre et communiquant aux utilisateurs les conditions d'utilisation appropriée en toute confiance de leur CCP et en obtenant par écrit leur acceptation de ces conditions;
- établissant, mettant en œuvre et communiquant aux utilisateurs les politiques et les procédures applicables à l'utilisation de leur CCP;
- établissant et communiquant ou faisant communiquer aux parties intéressées, y compris les utilisateurs et les parties qui s'y fient, toutes les limites applicables aux jugements, aux décisions ou aux règlements à leur détriment résultant de l'utilisation de ces CCP.

4.4 Faire en sorte que les dépôts soient à jour et interutilisables, en:

- faisant en sorte que les CCP et les LCR soient publiés dans un dépôt commodément accessible pour qu'on puisse vérifier la validité des listes;
- veillant à ce que les renseignements concernant les CCP et les LCR figurant dans le dépôt soient tous à jour;
- faisant en sorte que leur dépôt soit interutilisable avec les autres dépôts ministériels et avec ceux des AC communes et qu'il soit enregistré auprès du registraire des dépôts, dans le cas d'une AC commune.

4.5 Mettre en œuvre des pratiques appropriées de gestion de l'information et des clés, en:

- élaborant des politiques et des procédures de gestion de l'information de manière appropriée lorsqu'on a recours au chiffrement. L'information devrait alors être gérée conformément à la Loi sur la protection des renseignements personnels, à la Loi sur l'accès à l'information, à la Loi sur la Bibliothèque et les Archives du Canada et aux autres lois et politiques pertinentes du gouvernement. On devrait accorder une attention particulière à la façon du ministère d'assurer l'accès aux données cryptées advenant des demandes d'accès à l'information ou de découverte électronique;
- s'il y a lieu, en conservant une copie des clés de confidentialité privées des utilisateurs pour fins de récupération des données, en avisant les utilisateurs qu'on a créé des copies de sauvegarde de leurs clés de confidentialité privées et en les avisant que le ministère y a accès;
- s'assurant d'obtenir le consentement des utilisateurs avant de faire des copies de sauvegarde de leurs clés de confidentialité privées;
- s'assurant qu'on n'accède pas aux clés de confidentialité privées des utilisateurs ou qu'on ne les communique pas sans leur consentement préalable ou sans que la loi ou une autorisation judiciaire ne l'exige ou le permette;
- s'assurant qu'ils ne conservent ni n'ont conservé dans quelque circonstance que ce soit une copie de clés de signatures numériques privées. (N.B. : la conservation de clés de signatures numériques privées dans des serveurs ministériels n'en est pas une conservation par le ministère, pourvu qu'elles restent sous le contrôle de l'utilisateur.)

5. Responsabilités et Services Des Organismes responsables de L'ICP

Cette rubrique est une description des rôles, des responsabilités et des services des organismes responsables du soutien de la gestion de l'ICP.

5.1 Secrétariat du Conseil du Trésor

Le SCT établit l'orientation pangouvernementale, fixe les priorités et officialise les exigences en matière de gestion de la sécurité et de l'identité, ce qui comprend :

- l'établissement et le maintien de la gouvernance de la sécurité interministérielle afin d'exercer la surveillance stratégique, d'assurer le leadership et de recommander les priorités nécessaires à l'établissement des normes et à la désignation des autorités nécessaires pour l'identification et l'authentification des individus, tant au GC qu'à l'extérieur du GC;
- l'accréditation des services communs du GC;
- la reconnaissance des AC aux fins décrites dans le Règlement sur les SES;
- la publication des lignes directrices à l'appui de la PSG et de ses directives.

5.2 Centre de la Sécurité des Télécommunications Canada

Le CSTC assure le leadership et la coordination des activités ministérielles visant à protéger les renseignements sur support électronique, ce qui comprend :

- la gestion et le maintien de la CCFICP aux fins de la certification réciproque des AC avec les autres AC du GC et avec les AC de l'extérieur du GC;
- la prestation d'avis et de conseils sur la certification des services partagés et communs de TI, les nouvelles technologies de sécurité des TI, la conception de l'architecture de la sécurité des TI, les solutions communes de sécurité des TI, y compris l'utilisation sûre de produits commerciaux normalisés, la conception de dispositifs de sécurité pour les systèmes et les réseaux ainsi que les évaluations de la posture de sécurité et de la vulnérabilité;
- la prestation d'avis et de conseils sur la certification des services de TI partagés, communs ou fédérés du GC;
- la prestation d'avis et de conseils aux ministères sur l'utilisation et l'application des produits de sécurité des TI, des dispositifs COMSEC, des mesures cryptographiques et de la gestion des clés.

5.3 Travaux Publics et Services Gouvernementaux Canada

TPSGC fournit des services communs de sécurité des TI et d'autres solutions permettant aux ministères d'échanger de l'information avec les citoyens, les entreprises et les employés, ce qui comprend :

- l'utilisation et le maintien de l'AC des services communs de GJI pour fins de délivrance de certificats numériques aux utilisateurs;
- l'utilisation et le maintien de l'AC du GED pour fins de délivrance de certificats numériques aux utilisateurs de l'extérieur du gouvernement;
- l'utilisation et le maintien du Service public de répertoire de frontière de GJI, qui sert de plaque tournante pour faciliter l'accès aux certificats et aux listes de certificats révoqués des AC réciproquement certifiées du GC.

6. Demandes de renseignements

Pour toute demande de renseignements au sujet du présent instrument de politique, veuillez communiquer avec la Division de la sécurité et gestion de l'identité.

Annexe A – Définitions

Autorité de certification (*Certification Authority*)
Entité responsable de l'utilisation d'un ou de plusieurs serveurs dont on se sert pour délivrer et gérer des certificats de clé publique et des listes de certificats révoqués.

Certificat de clé publique (*Public Key Certificate*)
Clé publique d'un utilisateur et autres renseignements portant une signature numérique avec la clé privée de l'autorité de certification qui l'a délivrée. La présentation du certificat est conforme à la Recommandation X.509 du Secteur de la normalisation des télécommunications(UIT-T) de l'Union internationale des télécommunications.

Clé (*Key*)
Séquence de symboles contrôlant des procédés de signature numérique et de chiffrement.

Dépôt (*Repository*)
Système permettant de stocker des certificats ou d'autres renseignements les concernant et d'y avoir accès. Un répertoire X.500 est un type de dépôt.

Énoncé de pratiques de certification (*Certification Practice Statement*)
Énoncé complet des mécanismes et des procédés qu'une autorité de certification emploie pour délivrer et gérer des certificats de clé publique conformément à une ou plusieurs politiques de certification. Si une autorité de certification adopte plus d'une politique de certification, l'énoncé de pratiques de certification doit contenir suffisamment d'information pour démontrer comment on satisfait aux exigences de ces politiques ou renvoyer à d'autres sources contenant cette information.

Entité (*Entity*)
Association d'au moins deux individus, entreprise, partenariat, fiducie, coentreprise ou autre forme d'organisation.

Fournisseur de services (*Service Provider*)
Individu ou entité offrant des services liés à un ou plusieurs aspects du fonctionnement d'une autorité de certification. Un fournisseur de services peut être un ministère ou une entité du secteur privé.

Individu (*Individual*)
Personne physique.

Infrastructure à clé publique (*Public Key Infrastructure*)
Ensemble de politiques, de procédés, de plateformes de serveurs, de logiciels et de postes de travail utilisés afin de délivrer et de gérer des certificats et des clés.

Liste de certificats révoqués (*Certificate Revocation List*)
Liste de certificats de clé publique délivrés par une autorité de certification, mais révoqués avant leur date d'expiration naturelle.

Politique de certification (*Certificate Policy*)
Ensemble de règles définies indiquant l'applicabilité d'un certificat de clé publique à une collectivité particulière et/ou une classe d'application donnée ayant des exigences de sécurité communes et précisant si le certificat de clé publique est valable pour une application ou une fin donnée. Une autorité de certification peut adopter plus d'une politique de certification.

Registraire des dépôts (*Registrar of repositories*)
Dans le cas des dépôts du gouvernement fédéral, Travaux publics et Services gouvernementaux Canada ou toute autre entité nommée par le Conseil canadien des normes pour s'acquitter des fonctions de l'Organisme canadien d'enregistrement de l'interconnexion de systèmes ouverts.

Signature électronique sécurisée (*Secure Electronic Signature*)
Signature résultant de l'application du procédé prescrit par le Règlement sur les SES.

Signature numérique (*Digital Signature*)
Résultat d'une transformation de données au moyen d'un système de clé chiffré faisant que l'individu ou l'entité qui reçoit les données initiales peut déterminer si la transformation a été faite à l'aide de la clé correspondant à la clé de l'individu ou de l'entité qui a réalisé la transformation et si les données ont été modifiées depuis la transformation.

Utilisateur (*User*)
Individu ou entité autorisés à qui un certificat est délivré.

Annexe B – Références

- Directive sur la gestion de la sécurité ministérielle (DGSM), Secrétariat du Conseil du Trésor du Canada, juillet 2009.
- Directive sur la gestion de l'identité (DGI), Secrétariat du Conseil du Trésor du Canada, juillet 2009.
- Guide ministériel pour l'adoption des services obligatoires de la Voie protégée, Direction du dirigeant principal de l'information, Secrétariat du Conseil du Trésor du Canada, octobre 2007.
- Politique sur la sécurité du gouvernement (PSG), Secrétariat du Conseil du Trésor du Canada, juillet 2009.
- Politique sur les services communs du GC, Secrétariat du Conseil du Trésor du Canada, octobre 2006.
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI), Secrétariat du Conseil du Trésor du Canada, mai 2004.
- Politiques sur le certificat de signature numérique et sur le certificat de confidentialité du GC (PDF 587 KO), version 4.0, avril 2006.
- Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)
- Loi sur la preuve au Canada
- Règlement sur les signatures électroniques sécurisées (Règlement sur les SES)
- Loi sur la Bibliothèque et les Archives du Canada
- Loi sur la protection des renseignements personnels

Annexe C – Acronymes

AC
Autorité de certification

CCFICP
Charnière fédérale canadienne de l'ICP
CCP
Certificat de clé publique
CST
Couche de sécurité pour le transport
DGI
Directive sur la gestion de l'identité
DGSM
Directive sur la gestion de la sécurité ministérielle
GC
Gouvernement du Canada
GED
Gouvernement en direct
GJI
Gestion des justificatifs internes
GLEE
Gestion sous licence d'Entrust Enterprise (éléments d'infrastructure partagés)
GSTI
Gestion de la sécurité des technologies de l'information
ICP
Infrastructure à clé publique
LCR
Liste de certificats révoqués
LPC
Loi sur la preuve au Canada
LPRPDE
Loi sur la protection des renseignements personnels et les documents électroniques
PSG
Politique sur la sécurité du gouvernement
SANIF
Service annuaire national de l'infrastructure fédérée
SES
Signature électronique sécurisée

Notes en bas de page

Note en bas de page fn1

PSG, 3.2.

Renvoi à la référence de la note en bas de page [1]

Note en bas de page fn2

DGSM, Annexe C.

Renvoi à la référence de la note en bas de page [2]

Note en bas de page fn3

DGSM, 6.1.7.

Renvoi à la référence de la note en bas de page [3]

Note en bas de page fn4

DGSM, 6.1.23.

Renvoi à la référence de la note en bas de page [4]

Note en bas de page fn5

GSTI, 9.6.

Renvoi à la référence de la note en bas de page [5]

Note en bas de page fn6

GSTI, 12.3.3.

Renvoi à la référence de la note en bas de page [6]