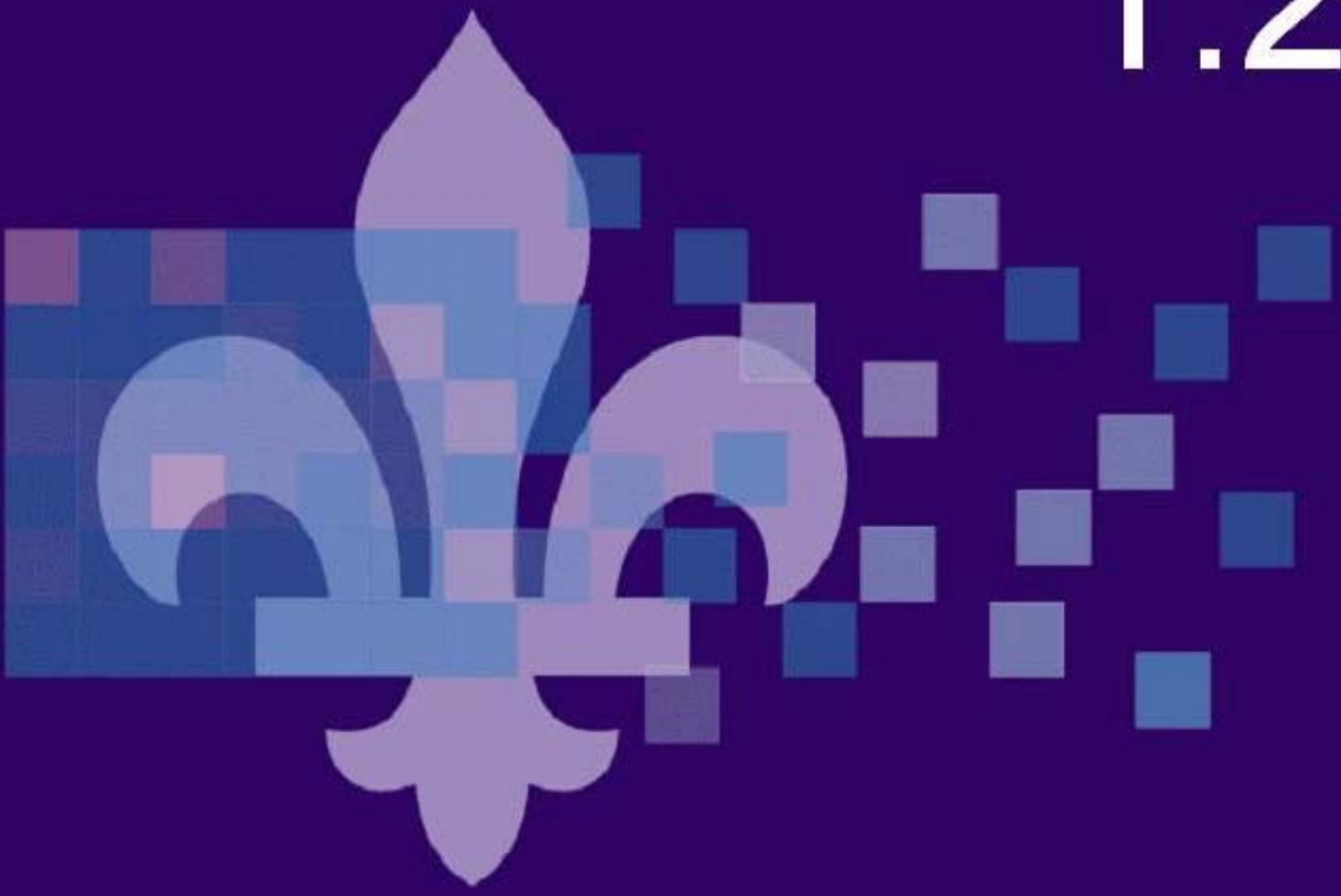
Directive sur les services de certification offerts par le gouvernement du Québec pendant la phase intérimaire

Version 1.2



Mars 2004
Identificateur d'objet de politique :
2.16.124.10.101.8.5.3.1

Québec

Secrétariat du Conseil du trésor

Directive sur les services de certification offerts par le gouvernement du Québec pendant la phase intérimaire

Version 1.2

identificateur d'objet de la politique : 2.16.124.10.101.8.5.3.1

Québec

TABLE DES MATIÈRES

CHAPITRE 1. DISPOSITIONS GÉNÉRALES 3
SECTION 1. OBJET ET CHAMP D'APPLICATION 3
§1. Objet 3
§2. Champ d'application 3
SECTION 2. DÉFINITIONS ET INTERPRÉTATION 4
§1. Définitions 4
§2. Interprétation 5
SECTION 3. LES RÔLES ET RESPONSABILITÉS DES INTERVENANTS DE L'ICPG 5
§1. Les services de certification et les services de répertoire 5
§2. Le gestionnaire des encadrements administratif et technique (GEAT) 6
§3. Le gestionnaire des clés et des certificats (GCC) 7
§4. Le gestionnaire de l'infrastructure opérationnelle (GIO) 8
§5. L'agent de vérification de l'identité (AVI) 9
§6. Le gestionnaire de l'utilisation (GU) 9
§7. L'abonné 10
§8. L'utilisateur de certificats 12
SECTION 4. L'UTILISATION DES CERTIFICATS ET DU RÉPERTOIRE 13
§1. Types de certificats et leurs niveaux de confiance 13
§2. Identificateur d'objet 13
§3. Limites à l'utilisation des clés, des certificats et du répertoire 14
CHAPITRE 2. PROCÉDURES EN MATIÈRE D'AUTHENTIFICATION ET DE VÉRIFICATION DE L'IDENTITÉ 15
SECTION 1. DÉLIVRANCE INITIALE DES PREMIÈRES CLÉS ET DES PREMIERS CERTIFICATS DE L'ICPG 15
§1. La vérification de l'identité initiale 15
§2. La vérification de l'identité du titulaire d'un certificat de niveau de confiance de base 15
§3. La vérification de l'identité du titulaire d'un certificat de niveau de confiance moyen 16
§4. La vérification de l'identité du titulaire d'un certificat de niveau de confiance élevé 17
§5. La vérification de l'identification des ministères, des organismes publics, des personnes morales, des sociétés, des associations, des groupes, des rôles, des dispositifs et des applications 17
§6. Le compte rendu de vérification 19
SECTION 2. AUTHENTIFICATION DE L'ABONNÉ PAR LE GCC 19
§1. Codes d'initialisation 19
§2. Preuve de la possession d'une clé privée 20
SECTION 3. LA VÉRIFICATION DE L'IDENTITÉ D'UN ABONNÉ DE MANIÈRE NON ÉQUIVOQUE 20
SECTION 4 . LE RENOUVELLEMENT DE CLÉS ET DE CERTIFICATS 21
SECTION 5. LA RÉCUPÉRATION DE CLÉS ET DE CERTIFICATS 21
SECTION 6. LA SUSPENSION D'UN CERTIFICAT 22
SECTION 7. L'ANNULATION D'UN CERTIFICAT 22
§1. Le retrait 22
§2. La révocation 22
SECTION 8. LA RECTIFICATION D'UN CERTIFICAT 22
SECTION 9. LA RÉATTRIBUTION D'UN CERTIFICAT À LA SUITE D'UNE ANNULATION OU D'UNE EXPIRATION 22

CHAPITRE 3. PROCÉDURES OPÉRATIONNELLES RELATIVES À LA DÉLIVRANCE ET À LA GESTION DES CLÉS ET DES CERTIFICATS 23
SECTION 1. DÉLIVRANCE INITIALE DE CLÉS ET DE CERTIFICATS DE L'ABONNÉ 23
§1. Personnes pouvant demander la délivrance 23
§2. Procédure de demande de délivrance 23
§3. Traitement d'une demande de délivrance 23
§4. Délai de traitement d'une demande de délivrance 24
§5. Acceptation de la demande et du certificat 25
§6. Avis de délivrance 25
SECTION 2. RENOUVELLEMENT DU CERTIFICAT D'UN ABONNÉ 25
§1. Personnes pouvant demander un renouvellement 25
§2. Traitement d'une demande de renouvellement 25
§3. Délai de traitement d'une demande de renouvellement 26
§4. Avis de renouvellement du certificat 26
SECTION 3. RÉCUPÉRATION DES CLÉS PRIVÉES DE CHIFFREMENT 26
§1. Personnes pouvant demander une récupération 26
§2. Circonstances pouvant entraîner la récupération 27
§3. Traitement d'une demande de récupération 27
§4. Délai de traitement d'une demande de récupération 28
SECTION 4. SUSPENSION DU CERTIFICAT D'UN ABONNÉ 28
§1. Personnes pouvant demander une suspension 28
§2. Circonstances pouvant entraîner une suspension 29
§3. Traitement d'une suspension 29
§4. Délai de traitement d'une demande suspension 29
SECTION 5. RETRAIT DU CERTIFICAT D'UN ABONNÉ (ANNULATION À LA DEMANDE D'UN ABONNÉ) 30
§1. Personne pouvant demander un retrait 30
§2. Circonstances pouvant entraîner le retrait 30
§3. Traitement d'une demande de retrait 30
§4. Délai de traitement d'une demande de retrait 31
SECTION 6. RÉVOCATION DU CERTIFICAT D'UN ABONNÉ (ANNULATION PAR LE GCC) 31
§1. Circonstances pouvant entraîner une révocation 31
§2. Traitement d'une révocation 31
§3. Délai de traitement d'une révocation 32
SECTION 7. RECTIFICATION DU CERTIFICAT D'UN ABONNÉ 33
§1. Personnes pouvant demander une rectification 33
§2. Circonstances pouvant entraîner une rectification 33
§3. Traitement d'une demande de rectification 33
§4. Délai de traitement d'une demande de rectification 34
SECTION 8. RÉATTRIBUTION À LA SUITE DE L'ANNULATION OU DE L'EXPIRATION D'UN CERTIFICAT 34
§1. Personne pouvant demander une réattribution 34
§2. Traitement d'une demande de réattribution 34
SECTION 9. PUBLICATION DU STATUT DU CERTIFICAT D'UN ABONNÉ 34
§1. Avis d'annulation du certificat d'un abonné 35
§2. Avis de suspension du certificat d'un abonné 35
§3. Avis d'archivage du certificat d'un abonné 35
SECTION 10. ANNULATION DU CERTIFICAT DU GCC 36

SECTION 11. PROCÉDURES DE VÉRIFICATION DE LA SÉCURITÉ INFORMATIQUE DU GCC 36
§1. Configuration initiale 36
§2. Types d'événements à consigner dans les registres de vérification 36
§3. Fréquence de traitement des registres de vérification 38
§4. Délai de conservation des registres de vérification 38
§5. Mesures de protection des registres de vérification 38
§6. Système de collecte des événements 38
§7. Avis à la suite d'un événement enregistré dans un registre de vérification 39
§8. Identification et traitement des vulnérabilités 39
SECTION 12. COPIE DE SÉCURITÉ DES DONNÉES 39
SECTION 13. CONSERVATION DES DONNÉES 39
§1. Délais de conservation des données 39
§2. Calendrier de conservation 40
§3. Lieu de conservation des données 40
SECTION 14. COMPROMISSION, CORRUPTION ET DÉSASTRE 40
§1. Corruption des équipements, des logiciels et des données 40
§2. Compromission de la confidentialité de la clé d'un GCC 40
§3. Compromission de la confidentialité de la clé de signature d'un AVI 41
§4. Recouvrement à la suite d'un désastre 41
SECTION 15. CESSATION DES ACTIVITÉS 41
§1. Cessation des activités d'un GCC 41
§2. Cessation des activités d'un AVI 42

CHAPITRE 4. MESURES DE SÉCURITÉ PHYSIQUE, ADMINISTRATIVE ET DU PERSONNEL 43

SECTION 1. MESURES DE SÉCURITÉ PHYSIQUE 43
§1. Mesures de sécurité physique pour le centre de gestion des clés et des certificats 43
§2. Mesures de sécurité physique pour le répertoire 44
§3. Mesures de sécurité physique pour l'AVI 44
§4. Mesures de sécurité physique pour les abonnés 45
§5. Alimentation électrique et climatisation 45
§6. Risques reliés aux dégâts d'eau 45
§7. Protection et prévention des incendies 45
§8. Conservation des supports magnétiques et physiques 45
§9. Destruction des supports 45
SECTION 2. MESURES DE SÉCURITÉ ADMINISTRATIVE ET OPÉRATIONNELLE 46
§1. Structure organisationnelle du centre de gestion 46
§2. Nombre de personnes requises pour effectuer les tâches 46
§3. Vérification des autorisations du personnel 46
SECTION 3. MESURES DE SÉCURITÉ DU PERSONNEL DU GCC 47
§1. Profil du personnel du GCC 47
§2. Formation 47
§3. Formation continue 48
§4. Sanctions à la suite d'actes non autorisés ou négligents 48
§5. Personnel contractuel 48
§6. Documentation fournie au personnel 48
SECTION 4. MESURES DE SÉCURITÉ RELATIVES AUX AVI 48

CHAPITRE 5. MESURES DE SÉCURITÉ TECHNIQUE 49
SECTION 1. GÉNÉRATION ET LIVRAISON DES CLÉS ET DES CERTIFICATS 49
§1. Génération de paires de clés 49
§2. Livraison des clés privées 49
§3. Livraison des clés publiques 49
§4. Livraison de la clé publique de vérification du GCC à l'abonné 50
§5. Longueur et période de validité des clés 50
§6. Génération matérielle et logicielle des clés 50
§7. Utilisation du champ d'extension « utilisation de la clé » (key usage) 50
§8. Génération des certificats de l'abonné 50
SECTION 2. PROTECTION DES CLÉS PRIVÉES DU GCC 50
§1. Clé privée de signature du GCC 50
§2. Clés du personnel du GCC 51
SECTION 3. PROTECTION DES CLÉS PRIVÉES DE L'ABONNÉ 51
§1. Conservation et support des clés 51
§2. Conservation par un tiers 51
§3. Transfert de la clé privée dans le module cryptographique 51
§4. Méthode d'activation 52
§5. Méthode de désactivation 52
§6. Méthode de destruction 52
SECTION 4. MESURES DE SÉCURITÉ DES ORDINATEURS 53
§1. Mesures de sécurité pour le GCC 53
§2. Mesures de sécurité pour l'AVI 54
SECTION 5. MESURES DE SÉCURITÉ DES RÉSEAUX 54
SECTION 6. MESURES DE CONTRÔLE D'INGÉNIERIE DES MODULES CRYPTOGRAPHIQUES 54
CHAPITRE 6. FORMAT ET CONTENU DES CERTIFICATS, DES LCA ET DES RÉPERTOIRES 55
SECTION 1. FORMAT ET CONTENU DES CERTIFICATS 55
§1. Format des certificats 55
§2. Contenu des certificats 55
§3. Formulation du nom distinctif 55
§4. Inscription de renseignements au certificat 56
§5. Interprétation et traitement des certificats 56
SECTION 2. FORMAT ET CONTENU DES LISTES DE CERTIFICATS ANNULÉS 56
SECTION 3. FORMAT ET CONTENU DU RÉPERTOIRE 57
SECTION 4. PÉRIODICITÉ ET PROCÉDURE DE MISE À JOUR DES CERTIFICATS, DES LCA ET DU RÉPERTOIRE 57
CHAPITRE 7. ADMINISTRATION DE LA DIRECTIVE 58
SECTION 1. PROCÉDURE DE DÉSIGNATION DES INTERVENANTS DE L'ICPG 58
§1. Gestionnaire des clés et des certificats 58
§2. Gestionnaire de l'utilisation 58
§3. Agent de vérification de l'identité 58
§4. Gestionnaire de l'infrastructure opérationnelle 58
§5. Perte de la désignation 59
SECTION 2. VÉRIFICATION DE CONFORMITÉ 59

§1. Vérification préalable à la désignation 59
§2. Vérification annuelle 59
§3. Vérification ponctuelle 59
§4. Conséquences de la vérification 59
SECTION 3. PROCÉDURES DE MODIFICATIONS DE LA DIRECTIVE 60
§1. Comité consultatif 60
§2. Modifications qui requièrent un nouvel identificateur d'objet 60
§3. Modifications qui requièrent un avis 60
§4. Version de la directive 61
SECTION 4. PUBLICATION DE LA DIRECTIVE 61
SECTION 5. SPÉCIFICATIONS TECHNIQUES POUR L'INFRASTRUCTURE À CLÉS PUBLIQUES GOUVERNEMENTALE 61
CHAPITRE 8. DISPOSITIONS DIVERSES 62
SECTION 1. PROTECTION DES RENSEIGNEMENTS PERSONNELS 62
SECTION 2. MÉCANISMES DE TRAITEMENT DES PLAINTES 62
SECTION 3. RÈGLEMENT DES LITIGES ENTRE LES INTERVENANTS DE L'ICPG 62
SECTION 4. RENSEIGNEMENTS DONT L'EXACTITUDE EST CONFIRMÉE 63
§1. Renseignements inscrits au certificat 63
§2. Renseignements inscrits au répertoire 63
SECTION 5. GARANTIES 63
SECTION 6. ENTENTE D'ABONNEMENT À L'ICPG 63
CHAPITRE 9. DISPOSITIONS TRANSITOIRES ET FINALES 65
SECTION 1. DISPOSITIONS TRANSITOIRES 65
§1. Secret partagé 65
§2. Numéro d'identificateur d'objet 65
§3. Évaluation des procédures de certification du GCC 65
SECTION 2. DISPOSITION FINALE 65

Directive sur les services de certification offerts par le gouvernement du Québec pendant la phase intérimaire

Préambule

Le Conseil du trésor décidait, en juin 1999, de doter le gouvernement du Québec d'une infrastructure à clés publiques gouvernementale (ICPG). L'ICPG est un système de gestion qui, en permettant notamment à des personnes de se reconnaître à distance, leur permet d'effectuer en toute sécurité des transactions électroniques et d'échanger de l'information de nature délicate. Cette façon d'assurer la sécurité des services électroniques permet aux ministères et aux organismes publics de mieux desservir leur clientèle tout en améliorant l'efficacité de leurs processus de travail.

L'ICPG permet notamment :

a) la confirmation de l'identité des personnes ou de l'identification des dispositifs agissant dans un environnement électronique;

b) l'intégrité des documents et des échanges électroniques;

c) la confidentialité des renseignements échangés ou conservés sur support informatique;

d) l'établissement d'un lien clair entre une personne et un document technologique ou entre une personne et une action.

L'ICPG est basée sur la délivrance et l'utilisation de paires de clés (également appelées « biclés »). Chacune des clés d'une paire est complémentaire et permet de déchiffrer ce qui a été chiffré avec l'autre. L'une des clés de la paire est certifiée et rendue publique (clé publique), l'autre est gardée secrète par son détenteur (clé privée).

La certification d'une clé publique est réalisée par un prestataire de services de certification dont le rôle premier est de délivrer un certificat contenant des informations préalablement vérifiées et confirmant l'identité de son détenteur. Un certificat peut servir à établir un ou plusieurs faits, notamment la confirmation de l'identité d'une personne ou, le cas échéant, l'identification d'une société, d'une association, d'un ministère ou d'un organisme public.

Le certificat de chiffrement d'un abonné de l'ICPG est rendu public par un prestataire de services de répertoire dont les fonctions consistent à inscrire dans un répertoire établi à cette fin tout certificat délivré et à confirmer la validité des certificats répertoriés.

Les phases de déploiement de l'ICPG

Le déploiement de l'ICPG a été prévu en deux phases. La première phase est intérimaire et vise à répondre aux besoins immédiats de certification s'adressant principalement à des employés, applications et dispositifs de l'État et à des mandataires du gouvernement ou de ses clients. Cette phase prendra fin lors du déploiement de la seconde phase dont le but consistera à déployer une solution permanente s'adressant à l'ensemble des personnes en relation avec l'État : employés, mandataires, citoyens et entreprises.

La présente directive vise à encadrer les services de certification offerts par le gouvernement du Québec pendant la phase intérimaire du déploiement de l'ICPG.

CHAPITRE 1. Dispositions générales

SECTION 1. Objet et champ d'application

§1. Objet

1. La présente directive énonce les règles applicables aux services de certification de l'infrastructure à clés publiques gouvernementale (ICPG) et aux services de répertoire qui y sont afférents afin d'assurer l'uniformité et la cohérence des exigences de certification au sein de l'Administration gouvernementale pendant la phase intérimaire du déploiement de l'ICPG.

2. Cette directive régit l'ensemble des processus de certification s'appliquant aux divers intervenants de l'ICPG, notamment :

   a) les exigences relatives à la délivrance, à la gestion et à l'utilisation des clés et des certificats;

   b) les exigences relatives à la vérification de l'identité;

   c) les exigences relatives à l'audit et à la désignation des intervenants de l'ICPG;

   d) les exigences relatives à la gestion de l'infrastructure matérielle et logicielle.

§2. Champ d'application

3. La présente directive s'applique au Conseil du trésor et à son Secrétariat, ainsi qu'aux ministères et organismes publics désignés pour agir comme gestionnaire des clés et des certificats ou comme gestionnaire de l'infrastructure opérationnelle de l'ICPG.

   Elle s'applique également à tous les ministères et organismes publics visés par l'article 64 de la Loi sur l'administration publique (L.R.Q., c. A-6.01) qui agissent en tant que gestionnaire de l'utilisation au sein de l'ICPG, à toute personne désignée comme agent de vérification de l'identité de l'ICPG ainsi qu'à toute personne visée par l'article 21 qui devient un abonné de l'ICPG.

   Tout autre organisme public peut adhérer volontairement à l'ICPG à titre de gestionnaire de l'utilisation, notamment les sociétés d'État et leurs filiales, les tribunaux au sens de la Loi sur les tribunaux judiciaires (L.R.Q., c. T-16), l'Assemblée nationale, les personnes nommées par cette dernière ainsi que les institutions et les organismes publics des réseaux de la Santé, de

l'Éducation et des municipalités. Ces organismes publics sont, dès leur adhésion, soumis aux droits et obligations d'un gestionnaire de l'utilisation en regard de l'application de la présente directive.

Malgré les alinéas précédents, la présente directive ne s'applique pas au ministère de la Justice en ce qui concerne les échanges électroniques effectués dans le cadre de l'utilisation du Registre des droits personnels et réels mobiliers.

SECTION 2. Définitions et interprétation

§1. Définitions

4. Dans la présente directive, on entend par :

« abonné » une personne physique partie à une entente d'abonnement visant l'obtention de clés et de certificats de l'ICPG;

« annulation » l'opération qui consiste à invalider un certificat à la suite d'un retrait ou d'une révocation;

« application ICP » un logiciel qui gère des clés et des certificats ou qui est en mesure d'utiliser les fonctions de l'ICPG, telles l'application du GCC, l'application de l'abonné et l'application de l'utilisateur;

« certificat » Un ensemble de données, dont le contenu minimal est défini à l'article 48 de la Loi concernant le cadre juridique des technologies de l'information (2001, c.32), signées à l'aide de la clé privée du prestataire de services de certification et servant à établir un ou plusieurs faits dont la confirmation de l'identité d'une personne ou, le cas échéant, l'identification d'une société, d'une association, d'un ministère ou d'un organisme public;

« identificateur d'objet » le numéro inscrit dans le certificat d'un abonné faisant référence à la présente directive et indiquant de quel type de certificat il s'agit;

« jeton cryptographique » un support matériel servant à générer et à emmagasiner la clé privée de signature d'un abonné, telle une carte à puce;

« niveau de confiance » le degré de certitude qu'une personne peut avoir quant à l'exactitude des informations inscrites dans un certificat;

« réattribution » l'opération qui consiste à générer de nouvelles clés et un nouveau certificat à la suite de l'annulation ou de l'expiration d'un certificat antérieur;

« rectification » l'opération qui consiste à modifier une information inscrite dans un certificat par la délivrance d'un nouveau certificat comportant l'information modifiée;

« récupération » l'opération déclenchée par le gestionnaire des clés et des certificats (GCC) ou par l'abonné et permettant à ce dernier de récupérer sa clé privée de déchiffrement lorsqu'elle ne peut plus être utilisée, notamment à la suite de l'oubli de son mot de passe, de la perte du fichier contenant ses clés ou d'un bris du poste de travail;

« renouvellement » l'opération automatisée effectuée par le GCC avant la date d'expiration d'un certificat valide et qui consiste à délivrer un nouveau certificat à un abonné;

« retrait » l'annulation d'un certificat effectuée par le GCC à la demande de l'abonné;

« révocation » l'annulation d'un certificat effectuée d'office par le GCC;

« secret partagé » une information connue de l'abonné et du GCC, tel un mot de passe, une information personnelle sur l'abonné ou un numéro d'identification personnel (NIP);

« suspension » l'opération qui consiste à enlever du répertoire le certificat de chiffrement d'un abonné et qui l'empêche d'utiliser ses clés et ses certificats;

« utilisateur » une personne qui agit en se fondant sur un renseignement inscrit au certificat d'un abonné de l'ICPG.

§2. Interprétation

5. La présente directive constitue un « énoncé de politique » au sens de l'article 52 de la Loi concernant le cadre juridique des technologies de l'information (2001, c. 32).

SECTION 3. Les rôles et responsabilités des intervenants de l'ICPG

§1. Les services de certification et les services de répertoire

6. Les services de certification offerts par le gouvernement du Québec en vertu de la présente directive font appel à la technologie de cryptographie asymétrique qui prévoit la délivrance de paires de clés et de certificats. Ces services sont assurés par quatre intervenants distincts dont les rôles et responsabilités sont définis dans la présente directive.

Ces quatre intervenants sont : le gestionnaire des encadrements administratif et technique, le gestionnaire des clés et des certificats, le gestionnaire de l'infrastructure opérationnelle et l'agent de vérification d'identité, lesquels, dans le cadre de leurs responsabilités respectives, agissent au nom du prestataire de services de certification.

7. Les services de répertoire offerts par le gouvernement du Québec en vertu de la présente directive sont afférents aux services de certification et sont assurés par trois intervenants distincts dont les rôles et responsabilités sont définis dans la présente directive.

Ces trois intervenants sont : le gestionnaire des encadrements administratif et technique, le gestionnaire des clés et des certificats et le gestionnaire de l'infrastructure opérationnelle, lesquels, dans le cadre de leurs responsabilités respectives, agissent au nom du prestataire de services de répertoire.

§2. Le gestionnaire des encadrements administratif et technique (GEAT)

8. Le Conseil du trésor assume la fonction de gestionnaire des encadrements administratif et technique (GEAT).

À ce titre, il a pour principales responsabilités :

a) d'assurer le maintien des niveaux de confiance des certificats délivrés dans le cadre de l'ICPG;

b) d'assurer la coordination et l'interopérabilité des gestes posés par les différents intervenants de l'ICPG, notamment par l'établissement de règles et de modalités de gestion applicables à l'ensemble de ces intervenants.

9. Le Conseil du trésor confie l'exécution des fonctions du GEAT à son Secrétariat, à l'exception des fonctions suivantes :

a) la désignation des GCC et des GIO;

b) la détermination, notamment en fonction d'une catégorisation de l'information effectuée par les GU, des types de certificats appropriés pour chaque catégorie d'information ainsi que des cas où l'utilisation de l'ICPG est obligatoire;

c) l'autorisation, sous réserve des exigences de la loi en matière d'ententes internationales et intergouvernementales, de conclure des ententes de reconnaissance avec d'autres prestataires de services de certification et l'interconnexion avec d'autres infrastructures à clés publiques qu'il juge opportunes et qui s'imposent alors à l'ensemble de l'ICPG.

§3. Le gestionnaire des clés et des certificats (GCC)

10. Un gestionnaire des clés et des certificats (GCC) est chargé d'administrer et d'opérer un service de gestion de clés et de certificats offert à l'ensemble des ministères et des organismes publics visés par la présente directive.

    À cette fin, le GCC est responsable de l'ensemble des aspects opérationnels et technologiques associés à la délivrance des clés et des certificats et aux opérations subséquentes reliées à leur cycle de vie, à l'exception de la vérification de l'identité initiale de l'abonné, laquelle relève de l'AVI.

11. La fonction de GCC consiste notamment à :

    a) mettre en place les mécanismes de communication permettant d'assurer la cohérence opérationnelle entre les différents intervenants de l'ICPG avec qui il collabore;

    b) s'assurer que les AVI avec qui il collabore respectent les exigences opérationnelles du GCC;

    c) délivrer des clés et des certificats et procéder aux opérations subséquentes sur ces derniers;

    d) mettre à la disposition de l'abonné, s'il y a lieu, des modules cryptographiques conformes aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale établies en vertu de l'article 244;

    e) maintenir le niveau de confiance des clés et des certificats par différents moyens de contrôle et par des mesures de sécurité s'appliquant aux volets opérationnel, administratif, physique et technologique relevant de son champ de responsabilités;

    f) planifier et assurer l'implantation, l'exploitation, l'entretien et l'évolution de l'infrastructure opérationnelle;

    g) participer aux activités du comité consultatif prévu à l'article 238.

12. Pour assumer ses fonctions, le GCC doit :

    a) ouvrir et mettre à jour des dossiers d'abonnés;

    b) distribuer les codes d'initialisation;

    c) respecter, selon les lois applicables, la confidentialité des données recueillies;

d) générer et délivrer des certificats de signature numérique ainsi que des paires de clés et des certificats de chiffrement, ainsi qu'apposer sa signature sur les certificats;

e) inscrire et publier dans un répertoire les certificats de chiffrement ainsi que l'information sur les certificats annulés;

f) effectuer toute opération subséquente sur les certificats;

g) s'assurer que la clé privée servant à apposer la signature du GCC sur les certificats et sur les listes de certificats annulés (LCA) ne sert qu'à cette fin;

h) préparer les ententes de service entre le GCC et les autres intervenants;

i) rendre opérationnelles les ententes de reconnaissance avec des prestataires de services de certification externes ou d'autres GCC;

j) élaborer une procédure de certification qui décrit les processus qu'il utilise dans la gestion du cycle de vie des clés et des certificats délivrés aux abonnés;

k) conserver les clés de déchiffrement;

l) s'assurer du respect des dispositions de la présente directive à l'intérieur de son champ de compétence.

13. Le GCC qui délivre des certificats de niveaux de confiance de base ou moyen peut déléguer à un GIO dûment désigné les fonctions autorisées par le GEAT.

§4. Le gestionnaire de l'infrastructure opérationnelle (GIO)

14. Un gestionnaire de l'infrastructure opérationnelle (GIO) assume les fonctions qui lui sont déléguées par un ou plusieurs GCC.

À cette fin, le GIO peut notamment assumer les fonctions suivantes :

a) assurer les activités techniques et opérationnelles soutenant le GCC;

b) voir à la sécurité des appareils et des logiciels utilisés par le GCC;

c) assurer le service technique à la clientèle;

d) développer, installer, opérer et entretenir les infrastructures matérielles et logicielles nécessaires pour soutenir le GCC.

15. Le GIO participe aux activités du comité consultatif prévu à l'article 238. Il doit également s'assurer du respect des dispositions de cette directive à l'intérieur de son champ de compétence.

§5. L'agent de vérification de l'identité (AVI)

16. Seule une personne physique désignée par le GEAT peut exercer la fonction d'agent de vérification de l'identité (AVI).

17. Les fonctions d'un AVI consistent notamment à :

    a) vérifier l'identité des abonnés et, s'il y a lieu, effectuer les autres vérifications prévues à la présente directive;

    b) expliquer et faire signer à l'abonné une entente d'abonnement;

    c) le cas échéant, conserver les ententes d'abonnement et les transmettre au GCC sur demande;

    d) fournir au GCC les coordonnées des abonnés ainsi que le secret partagé, le cas échéant;

    e) respecter les exigences opérationnelles du GCC;

    f) le cas échéant, conserver, selon les lois applicables, les renseignements recueillis dans le cadre de la vérification de l'identité et classifier ces renseignements de manière à pouvoir les retracer sur demande en tout temps;

    g) respecter la confidentialité des données recueillies selon les lois applicables, notamment le secret partagé, le cas échéant;

    h) protéger ses équipements contre toute atteinte à leur sécurité et à leur intégrité;

    i) protéger, le cas échéant, le code d'initialisation qui lui est transmis par le GCC jusqu'à la remise à l'abonné et informer le GCC de la date de cette remise;

    j) délivrer, le cas échéant, des jetons cryptographiques et assister l'abonné lors du processus de création et d'initialisation des clés.

§6. Le gestionnaire de l'utilisation (GU)

18. Le gestionnaire de l'utilisation (GU) autorise l'attribution de certificats et en gère l'usage à l'intérieur de son champ de responsabilités.

19. La fonction d'un GU consiste à :

a) adapter ses processus d'affaires à l'utilisation de clés et de certificats de l'ICPG;

b) déterminer, conformément aux normes gouvernementales, les niveaux de confiance requis pour chacun des processus d'affaires concernés;

c) déterminer quelles personnes pourront obtenir et utiliser des clés et des certificats;

d) gérer les accès à ses applications informatiques;

e) intégrer dans ses applications informatiques les fonctionnalités offertes par l'ICPG conformément aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale et toute autre spécification technique ou fonctionnelle du GEAT ou du GCC;

f) déterminer et vérifier les usages et les procédures d'utilisation des clés et des certificats au sein de ses processus d'affaires;

g) informer les abonnés des conséquences de l'utilisation de clés et de certificats de l'ICPG en matière de protection des renseignements personnels, notamment du fait que les informations inscrites au certificat seront rendues publiques;

h) informer les abonnés des utilisations autorisées et leur offrir un soutien;

i) s'assurer que les abonnés disposent des moyens et des outils nécessaires pour respecter leurs obligations en vertu de la présente directive, notamment en ce qui concerne l'obligation de préserver l'intégrité et la confidentialité de leurs clés privées;

j) s'assurer que les abonnés utilisent des modules cryptographiques et des applications ICP conformes aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale;

k) informer le GCC de tout élément dont il a connaissance pouvant mener à la modification, à la récupération, à la suspension ou à l'annulation d'un certificat;

l) s'assurer du respect des dispositions de la présente directive à l'intérieur de son champ de responsabilité.

§7. L'abonné

20. Sous réserve des dispositions de l'article 73, une personne est abonnée à l'ICPG dès lors qu'elle signe une entente d'abonnement visant l'obtention de clés et de certificats de l'ICPG.

21. Peut être un abonné de l'ICPG :

    a) un membre du personnel d'un GU, y compris un ministre ou le dirigeant d'un organisme public;

    b) un individu mandataire ou partenaire d'un GU;

    c) un membre du personnel d'une organisation mandataire ou partenaire d'un GU;

    d) un individu agissant dans le cadre d'un contrat de service avec un GU ou avec le mandataire ou le partenaire d'un GU, et dont les attributions nécessitent de communiquer de manière électronique avec ce GU, ce mandataire ou ce partenaire;

    e) un individu désigné par le GEAT pour agir comme AVI;

    f) un individu qui, en vertu de la Loi sur la transparence et l'éthique en matière de lobbyisme (2002, c.23), présente une déclaration ou un autre avis au registre des lobbyistes, ainsi que la personne nommée par l'Assemblée nationale pour agir à titre de commissaire au lobbyisme et le personnel autorisé par ce dernier;

    g) un juge de la Cour d'appel, de la Cour supérieure, de la Cour du Québec ou d'une Cour municipale, un membre nommé au Tribunal administratif du Québec ou un commissaire de la Commission des relations de travail;

    h) un député siégeant à l'Assemblée nationale;

    i) un membre d'un conseil municipal, ainsi que toute personne nommée par le conseil pour être membre d'une commission, d'un comité, d'un bureau de délégués ou de tout autre regroupement de même nature.

22. L'abonné peut être titulaire d'un certificat qui permet de confirmer son identité. Le certificat peut également servir à établir un lien entre lui et un ministère, un organisme public, une personne morale, une société ou une association.

    Un abonné peut également être titulaire d'un certificat qui sera affecté à un groupe, à un rôle, à un dispositif ou à une application au sein du gouvernement, d'une personne morale, d'une société ou d'une association. Toutefois, l'abonné ne peut ainsi affecter un certificat que dans la mesure où la responsabilité des processus d'affaires visés lui est imputable. Une telle affectation n'a pas pour effet de décharger l'abonné de sa responsabilité à l'égard de l'utilisation du certificat.

23. L'abonné a notamment la responsabilité de :

a) fournir à l'AVI les renseignements exacts et produire les pièces et documents pertinents;

b) utiliser ses clés adéquatement pour les seules fins autorisées;

c) utiliser ses équipements de façon sécuritaire, notamment vérifier que ses clés privées sont désactivées avant de quitter son poste de travail;

d) s'assurer de la confidentialité de tout code d'initialisation ou secret partagé;

e) s'assurer de la sécurité et de la confidentialité de ses clés privées, notamment par la protection de la donnée d'activation permettant d'utiliser ses clés privées, tel un mot de passe;

f) s'assurer que ses clés privées ne sont utilisées que par lui ou, lorsque les clés sont affectées à un dispositif, à une application, à un groupe ou à un rôle, par une personne autorisée;

g) aviser immédiatement le GU ou le GCC de tout changement aux renseignements inscrits à ses certificats ou lorsque la confidentialité de ses clés privées a été compromise;

h) ne pas utiliser une clé privée lorsque le certificat correspondant est annulé ou suspendu;

i) respecter l'entente d'abonnement qui le lie avec l'ICPG.

§8. L'utilisateur de certificats

24. Est un utilisateur de l'ICPG :

a) l'abonné de l'ICPG, lorsqu'il agit en se fondant sur le certificat d'un autre abonné de l'ICPG;

b) l'abonné d'un prestataire de services de certification reconnu par l'ICPG dans le cadre d'une entente de reconnaissance.

25. L'utilisateur a notamment la responsabilité de :

a) vérifier la validité d'un certificat avant de l'utiliser, notamment en s'assurant que le certificat n'est pas périmé, annulé ou suspendu et qu'il ne comporte pas la mention « certificat d'essai » ou toute autre mention de même nature indiquant qu'on ne peut raisonnablement s'y fier;

b) vérifier la portée d'un certificat avant de l'utiliser, notamment en s'assurant que le type de certificat est approprié pour l'usage qu'il désire en faire, conformément aux indications de la section 4 du présent chapitre;

c) vérifier la signature du GCC sur le certificat;

d) utiliser les certificats à l'aide d'applications ICP répondant aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

26. Les droits et obligations d'un utilisateur abonné à l'ICPG sont régis par la présente directive, alors que les droits et obligations d'un utilisateur abonné à un service de certification externe sont régis par l'énoncé de politique de certification du prestataire de ce service.

SECTION 4. L'utilisation des certificats et du répertoire

§1. Types de certificats et leurs niveaux de confiance

27. Le prestataire de services de certification peut, en vertu de la présente directive, délivrer les types de certificats suivants :

a) Certificats de signature numérique – niveau de confiance de base;

b) Certificats de signature numérique – niveau de confiance moyen;

c) Certificats de signature numérique – niveau de confiance élevé;

d) Certificats de chiffrement – niveau de confiance de base;

e) Certificats de chiffrement – niveau de confiance moyen;

f) Certificats de chiffrement – niveau de confiance élevé.

§2. Identificateur d'objet

28. La présente directive détermine, pour chacun des types de certificats, un ensemble de règles qui lui sont applicables. Chaque type de certificats est également identifié par un identificateur d'objet.

29. Les identificateurs d'objet pour les différents certificats pouvant être délivrés en vertu de la présente directive sont les suivants :

Types de certificats	Identificateurs d'objet
Signature numérique – niveau de confiance de base	2.16.124.10.101.8.5.3.1.2.20
Signature numérique – niveau de confiance moyen	2.16.124.10.101.8.5.3.1.2.30
Signature numérique – niveau de confiance élevé	2.16.124.10.101.8.5.3.1.2.40
Chiffrement – niveau de confiance de base	2.16.124.10.101.8.5.3.1.1.20
Chiffrement – niveau de confiance moyen	2.16.124.10.101.8.5.3.1.1.30
Chiffrement – niveau de confiance élevé	2.16.124.10.101.8.5.3.1.1.40

30. L'utilisateur qui agit en se fondant sur un certificat doit vérifier que l'identificateur d'objet indiqué dans le certificat correspond, selon la présente directive, à un niveau de confiance acceptable pour l'utilisation qu'il désire en faire.

§3. Limites à l'utilisation des clés, des certificats et du répertoire

31. Les clés et les certificats délivrés dans le cadre de l'ICPG ne peuvent être utilisés que dans le cadre de transactions, d'applications ou d'échanges électroniques avec le gouvernement du Québec ou avec tout autre organisme public désigné comme GU. La présente directive n'impose aucune limite relative à la valeur d'une transaction dans le cadre de laquelle les clés et les certificats peuvent être utilisés.

32. Les inscriptions contenues au répertoire ne peuvent être utilisées par les abonnés ou les utilisateurs que pour accéder au certificat de chiffrement d'un abonné ou pour accéder aux listes de certificats annulés (LCA).

33. Tout autre renseignement concernant les limites d'utilisation des clés et des certificats de l'ICPG ou du répertoire, lorsqu'il est disponible mais non encore inscrit au certificat ou au répertoire, doit être publié sur le site Web du Secrétariat du Conseil du trésor (www.tresor.gouv.qc.ca), tel qu'indiqué à l'article 243.

CHAPITRE 2. Procédures en matière d'authentification et de vérification de l'identité

34. Le présent chapitre énonce les règles applicables en matière d'authentification et de vérification de l'identité des abonnés tout au long du cycle de vie des certificats.

SECTION 1. Délivrance initiale des premières clés et des premiers certificats de l'ICPG

§1. La vérification de l'identité initiale

35. La vérification de l'identité d'un abonné consiste à en établir l'identité selon la procédure prescrite. Le cas échéant, la procédure de vérification de cette identité peut également servir à établir l'existence et l'identification d'un ministère, d'un organisme public, d'une personne morale, d'une société, d'une association, d'un groupe, d'un rôle, d'un dispositif ou d'une application, ainsi que son lien avec l'abonné.

36. L'AVI doit être désigné par le GEAT. Un AVI désigné pour effectuer la vérification d'identité pour un niveau de confiance donné peut également vérifier l'identité pour un niveau de confiance inférieur.

37. Toute personne qui désire s'abonner à l'ICPG doit faire vérifier son identité par un AVI dûment désigné.

38. Toute information obtenue par un AVI dans le cadre d'une vérification d'identité doit être recueillie, manipulée et conservée dans le respect des lois, notamment celles applicables en matière de protection des renseignements personnels.

39. Le GEAT peut prescrire les modalités relatives à la vérification d'identité pour toute catégorie d'abonné, tout type de certificat ou toute catégorie d'AVI.

§2. La vérification de l'identité du titulaire d'un certificat de niveau de confiance de base

40. La personne qui désire obtenir des clés et des certificats de niveau de confiance de base doit présenter une demande à l'AVI. Le demandeur doit également présenter à l'AVI un document avec photo confirmant son identité, émanant d'une autorité gouvernementale reconnue. L'AVI conserve les renseignements permettant de constater qu'il a vérifié l'identité du demandeur et les communique au GCC sur demande.

Cependant, si l'AVI avait autrement établi l'identité du demandeur de manière suffisante préalablement à la demande de délivrance initiale, il peut recourir à cette information pour fonder sa vérification.

41. *(Abrogé).*

42. L'AVI doit refuser les documents présentés lorsqu'il doute de la validité ou de l'authenticité de ces documents. Il appartient à l'AVI de se satisfaire ou non des pièces justificatives fournies par le demandeur pour prouver qu'il est bien celui qu'il prétend être.

§3. *La vérification de l'identité du titulaire d'un certificat de niveau de confiance moyen*

43. La personne qui désire obtenir des clés et des certificats de niveau de confiance moyen doit présenter une demande à l'AVI. Cette demande peut être présentée en personne ou à distance.

43.1. L'AVI qui vérifie l'identité d'un demandeur en sa présence physique doit vérifier deux documents confirmant l'identité du demandeur, émanant d'une autorité gouvernementale reconnue, dont l'un avec photo.

Lorsque le demandeur est un juge de la Cour d'appel, de la Cour supérieure ou de la Cour du Québec, l'AVI peut vérifier son identité en comparant la signature manuscrite apposée sur la demande avec un spécimen de signature recueilli lors de son assermentation ou à un autre moment par le juge en chef et que ce spécimen de signature ait été conservé de manière sécuritaire.

44. L'AVI doit refuser les preuves d'identité présentées lorsqu'il doute de leur validité ou de leur authenticité. Il appartient à l'AVI de se satisfaire ou non des pièces justificatives fournies par le demandeur pour prouver qu'il est bien celui qu'il prétend être.

45. L'AVI doit conserver les renseignements permettant de constater qu'il a vérifié l'identité du demandeur et doit les communiquer au GCC sur demande.

Ces renseignements sont :

a) le type de preuve d'identité vérifiée;

b) le cas échéant, la date de création, la date d'émission ou la date d'expiration des preuves vérifiées.

§4. *La vérification de l'identité du titulaire d'un certificat de niveau de confiance élevé*

46. La personne qui désire obtenir des clés et des certificats de niveau de confiance élevé doit présenter en personne une demande à l'AVI. Le demandeur doit également présenter à l'AVI deux documents confirmant son identité, émanant d'une autorité gouvernementale reconnue, dont l'un avec photo.

47. L'AVI peut, à sa discrétion, demander tout autre document confirmant l'identité du demandeur ou effectuer toute autre vérification qu'il juge appropriée. Il doit refuser les documents présentés lorsqu'il doute de la validité ou de l'authenticité de ces documents. Il appartient à l'AVI de se satisfaire ou non des pièces justificatives fournies par le demandeur pour prouver qu'il est bien celui qu'il prétend être.

48. L'AVI doit conserver les renseignements permettant de constater qu'il a vérifié l'identité du demandeur et doit les communiquer au GCC sur demande.

Ces renseignements sont :

- le type de preuve d'identité vérifiée;
- le cas échéant, la date de création, la date d'émission ou la date d'expiration des preuves vérifiées.

§5. La vérification de l'identification des ministères, des organismes publics, des personnes morales, des sociétés, des associations, des groupes, des rôles, des dispositifs et des applications

49. Lorsque l'identification ou l'acronyme d'un ministère ou d'un organisme public doit être inscrit dans le certificat d'un abonné, l'AVI doit, en plus de vérifier l'identité du titulaire :

a) vérifier l'existence et l'identification du ministère ou de l'organisme public;

b) s'assurer que l'abonné est un membre du personnel du ministère ou de l'organisme public ou qu'il est autorisé à agir en son nom, et qu'il est autorisé à être titulaire d'un certificat comportant l'identification ou l'acronyme du ministère ou de l'organisme public.

L'AVI peut effectuer les vérifications prévues au présent article par tout moyen qu'il juge approprié, notamment par la consultation d'un document public tel une loi ou un décret ou par l'obtention d'une déclaration signée par un représentant autorisé en vertu du règlement sur la

délégation de signature en vigueur dans ce ministère ou cet organisme public ou en vertu de tout autre document équivalent dont la publicité est assurée.

50. Lorsque l'identification d'une personne morale, d'une société ou d'une association doit être inscrite dans le certificat, l'AVI doit, en plus de vérifier l'identité du titulaire :

a) vérifier l'existence et l'identification de la personne morale, de la société ou de l'association, notamment par la vérification des informations publiées sur le registre prévu à la Loi sur la publicité légale des entreprises individuelles, des sociétés et des personnes morales (L.R.Q. c. P-45) ou par la vérification de tout autre document procurant une certitude équivalente;

b) obtenir de l'abonné un document attestant qu'il est autorisé à représenter la personne morale, la société ou l'association et qu'il est autorisé à être titulaire d'un certificat comportant l'identification de cette organisation.

En outre de ces vérifications, l'AVI peut obtenir toute autre preuve suffisante afin d'établir l'exactitude de l'identification de la personne morale, de la société ou de l'association.

51. Lorsque les clés et les certificats sont affectés à un groupe, à un rôle, à un dispositif ou à une application au sein du gouvernement, l'abonné doit également produire une déclaration signée par un représentant autorisé en vertu du règlement sur la délégation de signature en vigueur dans le ministère ou l'organisme public visé ou en vertu de tout autre document équivalent dont la publicité est assurée. La déclaration doit indiquer l'identification du groupe, du rôle, du dispositif ou de l'application visé et doit indiquer que l'abonné est autorisé à lui affecter son certificat.

52. Lorsque les clés et les certificats doivent être affectés à un groupe, à un rôle, à un dispositif ou à une application au sein d'une personne morale, d'une société ou d'une association, l'abonné doit produire une déclaration signée par une personne autorisée de cette organisation. La déclaration doit indiquer l'identification du groupe, du rôle, du dispositif ou de l'application visé et doit indiquer que l'abonné est autorisé à lui affecter son certificat.

53. L'AVI doit conserver une copie de tout document qui lui est présenté pour effectuer la vérification prévue à la présente sous-section. Il doit également conserver une preuve de la vérification de tout fait qui lui a permis de déterminer, de manière suffisante, l'identification du ministère, de l'organisme public, de la personne morale, de la société, de l'association, du groupe, du rôle, du dispositif ou de l'application visé.

§6. *Le compte rendu de vérification*

54. L'AVI doit dresser un compte rendu de sa vérification selon les exigences du GCC avec lequel il collabore. Ce compte rendu doit comporter, au moins :

    a) le nom du demandeur, tel que vérifié suivant les prescriptions de la présente section;

    b) le fait que la vérification d'identité ait été faite ou non en la présence physique du demandeur;

    c) les autres renseignements vérifiés, le cas échéant;

    d) le nom du GU qui a autorisé la délivrance du certificat;

    e) la date du compte rendu;

    f) le nom et la signature de l'AVI.

55. Lorsque l'original du compte rendu de vérification n'est pas transmis au GCC, l'AVI doit prendre les mesures nécessaires afin d'en assurer la conservation sécuritaire et en produire une copie sur demande du GEAT ou du GCC.

SECTION 2. Authentification de l'abonné par le GCC

§1. *Codes d'initialisation*

56. Afin de s'assurer que les clés de chiffrement et les certificats signés sont transmis à la bonne personne, le GCC doit remettre de manière sécuritaire deux codes d'initialisation à l'abonné. Celui-ci doit ensuite utiliser ces codes pour s'identifier en ligne auprès de l'application du GCC, laquelle vérifie l'appariement des codes avant de procéder à l'échange de clés et de certificats.

57. Le GCC doit remettre à l'abonné chacun des codes d'initialisation par un moyen différent, par exemple :

    a) la transmission par courrier électronique;

    b) la transmission par courrier régulier;

    c) la remise sécuritaire à l'AVI afin qu'il remette le code en main propre à l'abonné;

d) la remise à l'abonné par téléphone après avoir vérifié son identité à l'aide d'un secret partagé conformément aux indications de la section 3 du présent chapitre.

Tout autre moyen d'authentification de l'abonné en ligne par l'application du GCC doit être conforme aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

§2. *Preuve de la possession d'une clé privée*

58. Avant de créer un certificat de signature et de le signer, l'application du GCC doit s'assurer que l'abonné est en possession de la clé privée associée à la clé publique reçue en vérifiant la signature apposée à un message par l'abonné avec sa clé privée. Cette exigence s'applique chaque fois qu'un certificat de signature est créé, soit lors de la délivrance initiale, d'un renouvellement, d'une récupération, d'une rectification ou d'une réattribution. Une telle vérification doit être effectuée conformément aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

Cette exigence ne s'applique pas à la clé de chiffrement.

SECTION 3. La vérification de l'identité d'un abonné de manière non équivoque

59. Le GCC peut, tout au long du cycle de vie des clés et des certificats, être tenu d'identifier un abonné de manière non équivoque, par exemple lorsqu'un abonné demande la récupération de sa clé de déchiffrement.

Sauf dans le cas de la délivrance initiale où la vérification de l'identité doit être effectuée de la manière décrite à la section 1 du présent chapitre, le GCC peut, pour identifier un abonné, recourir aux méthodes de vérification d'identité décrites à la présente section.

60. Sauf dans le cas où la confidentialité de la clé de signature d'un abonné a été compromise, celui-ci peut prouver son identité au GCC en signant un message à l'aide de sa clé privée de signature.

Lorsque le détenteur d'un certificat de niveau de confiance de base présente au GCC une demande sur support papier, le GCC peut vérifier son identité de manière non équivoque en comparant sa signature manuscrite à la signature apposée à l'entente d'abonnement.

61. Un secret partagé peut être utilisé entre un GCC et un abonné comme moyen de vérification de l'identité non équivoque si le secret a préalablement été transmis par l'abonné au GCC à l'aide d'un message signé et chiffré.

62. Un secret partagé transmis au GCC par l'AVI peut également être utilisé si les conditions suivantes sont remplies :

a) le secret partagé a été recueilli par l'AVI lors du processus de vérification de l'identité;

b) le secret partagé a été transmis au GCC par l'AVI à l'aide d'un message signé et chiffré;

c) le GCC a demandé à l'abonné de changer le secret partagé dès qu'il a été utilisé une première fois pour identifier l'abonné de manière non équivoque.

63. Lorsque ni la vérification par signature, ni la vérification par secret partagé ne peut être utilisée par le GCC, la vérification de l'identité de l'abonné doit être effectuée par un AVI, de la même manière que pour la délivrance initiale, selon la procédure décrite à la section 1 du présent chapitre.

64. L'identité du GU peut être vérifiée par le GCC de la même manière que pour l'abonné selon les méthodes prévues à la présente section. Facultativement, si le GU transmet une demande au GCC sur support papier, son représentant autorisé peut prouver son identité en apposant sa signature sur la demande.

SECTION 4 . Le renouvellement de clés et de certificats

65. La vérification de l'identité de l'abonné lors d'un renouvellement doit être effectuée par l'application du GCC qui vérifie la signature numérique créée par la clé privée de signature de l'abonné, le tout conformément aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

SECTION 5. La récupération de clés et de certificats

66. Le GCC doit vérifier d'une manière non équivoque l'identité de l'abonné qui demande une récupération. Lorsque des codes d'initialisation doivent être transmis de nouveau, ils doivent l'être de la même manière que celle prévue à l'article 57.

67. Lors d'une demande de récupération provenant d'un responsable de l'accès aux documents nommé en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q. c. A-2.1) ou d'une ordonnance du tribunal, le GCC doit s'assurer de remettre la clé privée de déchiffrement à la personne désignée par le responsable de l'accès aux documents ou par l'ordonnance du tribunal.

SECTION 6. La suspension d'un certificat

68. Le GCC doit vérifier d'une manière non équivoque l'identité de la personne qui demande la suspension d'un certificat.

SECTION 7. L'annulation d'un certificat

§1. Le retrait

69. Le GCC doit vérifier d'une manière non équivoque l'identité de la personne qui demande le retrait d'un certificat.

§2. *La révocation*

70. La révocation est toujours effectuée d'office par le GCC. Aucune vérification d'identité n'est requise.

SECTION 8. La rectification d'un certificat

71. Le GCC doit vérifier d'une manière non équivoque l'identité de la personne qui demande la rectification d'un certificat.

SECTION 9. La réattribution d'un certificat à la suite d'une annulation ou d'une expiration

72. Lorsqu'une personne demande une réattribution à la suite de l'annulation ou de l'expiration d'un certificat, le GCC doit vérifier l'identité du requérant d'une manière non équivoque et s'assurer que les informations inscrites à ce certificat sont toujours exactes. Cependant, lorsque l'annulation ou l'expiration a eu lieu depuis plus de six mois, la vérification d'identité doit être effectuée de la même manière que pour la délivrance initiale, selon la procédure décrite à la section 1 du présent chapitre.

    Lorsque des codes d'initialisation doivent être remis de nouveau, ils doivent l'être de la manière prévue à l'article 57.

CHAPITRE 3. Procédures opérationnelles relatives à la délivrance et à la gestion des clés et des certificats

SECTION 1. Délivrance initiale de clés et de certificats de l'abonné

§1. Personnes pouvant demander la délivrance

73. Seules les personnes autorisées par un GU peuvent être abonnées de l'ICPG et demander la délivrance de clés et de certificats.

§2. Procédure de demande de délivrance

74. Toute personne visée à l'article 21 qui désire obtenir des clés et des certificats doit suivre la procédure suivante :

a) faire une demande de délivrance en indiquant :

i) son nom,

ii) le cas échéant, l'identification ou l'acronyme du ministère, de l'organisme public, de la personne morale, de la société ou de l'association qui doit apparaître à son certificat,

iii) le cas échéant, l'identification du groupe, du rôle, du dispositif ou de l'application qui doit apparaître à son certificat,

iv) le nom du GU qui a autorisé la délivrance des clés et des certificats;

b) signer l'entente d'abonnement à l'ICPG comportant les termes et conditions s'appliquant aux clés et certificats ainsi qu'à leur usage;

c) fournir les preuves et les informations requises par l'AVI.

§3. Traitement d'une demande de délivrance

75. Lors du traitement d'une demande de délivrance, le GCC doit :

a) constater l'approbation du GU;

b) vérifier la conformité de la demande, notamment que toutes les informations prescrites sont présentes et que l'AVI possède les pouvoirs requis;

c) vérifier la confirmation de la vérification de l'identité par l'AVI;

c) inscrire l'abonné dans le répertoire et générer ses codes d'initialisation;

d) remettre les codes d'initialisation à l'abonné de la manière prévue à l'article 57.

76. Afin de compléter le processus de délivrance, l'abonné doit utiliser une application ICP qui génère et transmet au GCC une clé publique de vérification de signature. À ce moment, le GCC doit :

a) authentifier l'abonné de la manière prévue à l'article 56;

b) vérifier, de la manière prévue à l'article 58, que l'abonné est en possession d'une clé privée de signature;

c) générer un certificat de signature pour l'abonné, y apposer sa signature et le lui transmettre;

d) créer les clés et le certificat de chiffrement de l'abonné, signer ce certificat, transmettre les clés et le certificat à l'abonné et publier ce certificat dans un répertoire accessible aux utilisateurs de l'ICPG;

e) s'assurer que le délai entre la création des codes d'initialisation et la création des clés et certificats n'excède pas le délai prévu à l'article 79.

77. Le GCC doit, dans le cadre de ses responsabilités, colliger et conserver tout document relatif au traitement d'une demande de délivrance ainsi que toutes actions subséquentes posées au regard d'une telle demande. Il doit également signer tout document en attestant la réalisation et en conserver copie.

§4. Délai de traitement d'une demande de délivrance

78. Il n'est prescrit aucun délai entre la réception d'une demande de certificat et la délivrance des clés à l'abonné.

79. Pour les certificats de niveaux de confiance de base et moyen, l'abonné doit utiliser ses codes d'initialisation et procéder à la création de ses clés et certificats dans un délai de 15 jours à compter de la génération de ces codes. S'il ne le fait pas dans le délai prescrit, l'abonné devra demander de nouveaux codes d'initialisation au GCC avant l'expiration d'un délai de six mois à compter de la génération des premiers codes d'initialisation. .

Dans le cas des certificats de niveau de confiance élevé, l'abonné doit, dans les locaux sécurisés de l'AVI, générer ses clés de signature dès la réception de ses codes d'initialisation.

§5. Acceptation de la demande et du certificat

80. En apposant sa signature sur le certificat de l'abonné, le GCC signifie son approbation complète et finale de la demande de délivrance de certificat.

§6. Avis de délivrance

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

82. Par l'inscription d'un certificat au répertoire, le GCC certifie qu'il a délivré un certificat à l'abonné et que l'abonné a accepté ce certificat.

83. En inscrivant un certificat de chiffrement dans le répertoire, le GCC certifie aussi qu'il a délivré un certificat de signature numérique à l'abonné nommé et que l'abonné a accepté ce certificat.

SECTION 2. Renouvellement du certificat d'un abonné

§1. Personnes pouvant demander un renouvellement

84. Le renouvellement d'un certificat de niveaux de confiance de base ou moyen est initié de manière automatisée par l'application de l'abonné, laquelle peut, avant la date d'expiration de la clé privée de signature, demander en ligne le renouvellement des clés et des certificats pour autant que le certificat correspondant soit toujours valide.

Les clés et les certificats de niveau de confiance élevé ne peuvent être renouvelés.

§2. Traitement d'une demande de renouvellement

85. Si la clé privée de signature de l'abonné est toujours valide, l'abonné doit utiliser une application ICP qui génère et transmet au GCC une clé publique de vérification de signature. À ce moment, le GCC doit :

a) vérifier, de la manière prévue à l'article 58, que l'abonné est en possession d'une clé privée de signature;

b) générer un certificat de signature pour l'abonné, apposer sa signature sur ce certificat et le lui transmettre;

c) créer les clés et le certificat de chiffrement de l'abonné, signer ce certificat, transmettre les clés et le certificat à l'abonné et publier ce certificat dans un répertoire accessible aux utilisateurs de l'ICPG.

86. Dans le cas où la durée de validité de la clé privée de signature est échue, le GCC doit, sur demande de l'abonné, procéder à une réattribution en observant les prescriptions de la section 8 du présent chapitre.

87. Le GCC doit, dans le cadre de ses responsabilités, colliger et conserver tout document relatif au traitement d'une demande de renouvellement ainsi que toute action subséquente posée au regard d'une telle demande. Il doit également signer tout document en attestant la réalisation et en conserver copie.

§3. Délai de traitement d'une demande de renouvellement

88. La demande de renouvellement est automatique et est traitée dès sa réception.

§4. Avis de renouvellement du certificat

89. Le GCC doit aviser l'abonné du renouvellement de ses clés et de ses certificats.

SECTION 3. Récupération des clés privées de chiffrement

§1. Personnes pouvant demander une récupération

90. Les personnes suivantes peuvent demander la récupération des clés privées de chiffrement d'un abonné :

a) l'abonné lui-même;

b) le responsable de l'accès aux documents des organismes publics ou de la protection des renseignements personnels nommé en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels;

c) toute personne autorisée à demander la récupération à la suite d'un jugement ayant l'autorité de la chose jugée rendu par un tribunal compétent.

§2. Circonstances pouvant entraîner la récupération

91. La récupération des clés privées de chiffrement d'un abonné peut être demandée lorsqu'il devient impossible d'y accéder, notamment en raison de la perte du mot de passe ou de la destruction des clés.

§3. Traitement d'une demande de récupération

92. Le GCC doit, dans le cas où la demande est formulée par un abonné :

a) vérifier, par un des moyens prévus aux articles 59 à 63, l'identité de l'abonné qui demande la récupération;

b) créer les codes d'initialisation et les remettre à l'abonné de la manière prévue à l'article 57;

c) annuler l'ancien certificat de signature de l'abonné.

93. Afin de compléter le processus de délivrance, l'abonné doit utiliser une application qui génère et transmet au GCC une clé publique de vérification de signature. Dans un tel cas, le GCC doit :

a) authentifier l'abonné de la manière prévue à l'article 56;

b) vérifier, de la manière prévue à l'article 58, que l'abonné est en possession d'une clé privée de signature;

c) générer un certificat de signature pour l'abonné, apposer sa signature sur ce certificat et le lui transmettre;

d) récupérer les clés et le certificat de chiffrement de l'abonné et les transmettre à l'abonné;

e) s'assurer que le délai entre la création des codes d'initialisation et la récupération n'excède pas le délai prévu à l'article 97.

94. Dans le cas où la demande émane d'un tiers autorisé en vertu de l'article 90 de la présente directive, le GCC doit :

a) s'assurer de la validité de la demande;

b) aviser l'abonné de la demande de récupération, sauf indication contraire du tribunal;

c) générer des codes d'initialisation et les utiliser pour créer un fichier contenant les clés et le certificat de chiffrement récupérés de l'abonné;

d) annuler, le cas échéant, tous les certificats de signature de l'abonné aussitôt la création du fichier de clés complétée;

e) remettre le fichier de clés et le mot de passe permettant de l'utiliser à la personne désignée par le responsable de l'accès aux documents ou par l'ordonnance du tribunal;

f) effacer de ses systèmes toute copie du fichier de clés ainsi créé;

g) annuler le certificat de chiffrement sur confirmation que les données ont été récupérées.

95. Le GCC doit, dans le cadre de ses responsabilités, colliger et conserver tout document relatif au traitement d'une demande de récupération ainsi que toute action subséquente posée au regard d'une telle demande. Il doit également signer tout document en attestant la réalisation et en conserver copie.

§4. Délai de traitement d'une demande de récupération

96. Le GCC doit débuter le traitement d'une demande de récupération dans un délai raisonnable.

97. Lorsque des codes d'initialisation sont transmis à l'abonné, la période entre la création des codes d'initialisation et la création des clés et certificats ne doit pas excéder 15 jours pour les certificats de niveaux de confiance de base et moyen.

Pour les certificats de niveau de confiance élevé, l'abonné doit, dans les locaux sécurisés de l'AVI, générer ses nouvelles clés dès la réception de ses codes d'initialisation.

SECTION 4. Suspension du certificat d'un abonné

§1. Personnes pouvant demander une suspension

98. L'abonné et le GU peuvent demander la suspension d'un certificat lorsque le GCC offre ce service. Le GCC doit également suspendre d'office un certificat lorsqu'il reçoit une information pouvant mener à une révocation.

§2. Circonstances pouvant entraîner une suspension

99. La procédure de suspension peut notamment être utilisée, tel que prévu à l'article 111, lors de la révocation d'un certificat pour permettre au GCC de vérifier si la révocation est justifiée. De manière facultative, elle peut également être utilisée par un GCC dans d'autres circonstances, notamment lorsqu'un abonné doit cesser l'utilisation de ses clés pour une période de temps déterminée.

§3. Traitement d'une suspension

100. Pour effectuer la suspension d'un certificat, le GCC doit :

a) vérifier l'identité du demandeur de manière non équivoque lorsque la suspension est demandée par un abonné ou un GU;

b) suspendre le certificat;

c) aviser l'abonné et le GU de la suspension du certificat;

d) lorsque la période de suspension est terminée, ou sur demande de l'abonné ou du GU, le GCC doit :

i) vérifier l'identité du demandeur de manière non équivoque lorsque la suspension est demandée par un abonné ou un GU;

ii) remettre en vigueur le certificat;

iii) aviser l'abonné et le GU de la remise en vigueur.

101. Le GCC doit, dans le cadre de ses responsabilités, colliger et conserver tout document relatif au traitement d'une suspension ainsi que toute action subséquente posée au regard de cette opération. Il doit également signer tout document en attestant la réalisation et en conserver copie.

§4. Délai de traitement d'une demande suspension

102. Le GCC qui reçoit une demande de suspension d'un abonné ou d'un GU doit en compléter le traitement dans les délais suivants :

a) dans les deux jours ouvrables qui suivent la date de la réception de la demande, dans le cas d'une demande de suspension d'un certificat de niveau de confiance de base;

b) dans un délai d'un jour ouvrable qui suit la date de la réception de la demande, dans le cas d'une demande de suspension d'un certificat de niveau de confiance moyen;

c) dès la réception de la demande, dans le cas d'une demande de suspension d'un certificat de niveau de confiance élevé.

SECTION 5. Retrait du certificat d'un abonné (annulation à la demande d'un abonné)

§1. Personne pouvant demander un retrait

103. Seul l'abonné peut demander le retrait de son certificat.

§2. Circonstances pouvant entraîner le retrait

104. L'abonné doit demander au GCC le retrait de son certificat lorsque :

a) l'affiliation de l'abonné, telle que vérifiée par l'AVI en vertu des articles 49 à 53, a changé ou l'information contenue dans le certificat n'est plus exacte;

b) l'abonné soupçonne que la confidentialité de la clé privée correspondante est compromise;

c) l'abonné ne désire plus utiliser ses clés ou qu'il n'en a plus besoin.

§3. Traitement d'une demande de retrait

105. Lorsqu'il reçoit une demande de retrait, le GCC doit :

a) vérifier l'identité de l'abonné d'une manière non équivoque;

b) annuler le certificat;

c) rendre publique l'annulation du certificat de la manière prévue à la section 9 du présent chapitre;

d) si le motif du retrait est la fin de l'abonnement, demander à l'abonné de détruire le fichier contenant ses clés privées, de réinitialiser son jeton cryptographique ou de le rapporter au GU ou, le cas échéant, au GCC.

106. Si de nouvelles clés et de nouveaux certificats sont requis, le GCC doit appliquer la procédure de réattribution.

107. Le GCC doit, dans le cadre de ses responsabilités, colliger et conserver tout document relatif au traitement d'une demande de retrait ainsi que toute action subséquente posée au regard d'une telle demande. Il doit également signer tout document en attestant la réalisation et en conserver copie.

§4. Délai de traitement d'une demande de retrait

108. Le GCC qui reçoit une demande de retrait doit en avoir complété le traitement dans les délais suivants :

a) dans les deux jours ouvrables qui suivent la date de la réception de la demande de retrait d'un certificat de niveau de confiance de base;

b) dans le délai d'un jour ouvrable qui suit la date de la réception de la demande de retrait d'un certificat de niveau de confiance moyen;

c) dès la réception de la demande, dans le cas d'une demande de retrait d'un certificat de niveau de confiance élevé.

SECTION 6. Révocation du certificat d'un abonné (annulation par le GCC)

109. Toute personne peut transmettre au GCC une information pouvant mener, selon les circonstances, à la révocation d'un certificat.

§1. Circonstances pouvant entraîner une révocation

110. Un certificat doit être révoqué lorsque :

a) l'affiliation de l'abonné, telle que vérifiée par l'AVI en vertu des articles 49 à 53, a changé ou l'information contenue dans le certificat n'est plus exacte;

b) la confidentialité de la clé privée correspondante est compromise ou qu'on soupçonne qu'elle l'est;

c) l'abonné ne respecte pas les conditions d'utilisation de ses clés et certificats;

d) tous les GU ont retiré à l'abonné l'autorisation d'utiliser ses clés et ses certificats.

§2. Traitement d'une révocation

111. Lorsqu'il reçoit une information pouvant mener à la révocation, le GCC doit :

a) vérifier l'identité de la personne qui transmet l'information;

b) suspendre temporairement le certificat visé;

c) aviser l'abonné de la suspension et lui accorder au moins 15 jours pour présenter ses observations;

d) déterminer si la révocation est justifiée;

e) remettre en vigueur le certificat ou l'annuler, selon le cas;

f) aviser l'abonné de la remise en vigueur ou de la révocation, selon le cas;

g) rendre publique l'annulation du certificat de la manière prévue à la section 9 du présent chapitre.

112. Si de nouvelles clés et de nouveaux certificats sont requis, le GCC doit appliquer la procédure de réattribution décrite à la section 8 du présent chapitre.

113. Le GCC doit, dans le cadre de ses responsabilités, colliger et conserver tout document relatif au traitement d'une révocation ainsi que toute action subséquente posée au regard de cette opération. Il doit également signer tout document en attestant la réalisation et en conserver copie.

§3. Délai de traitement d'une révocation

114. Le GCC doit commencer le traitement d'une révocation :

a) dans les deux jours ouvrables suivant la réception de l'information qui enclenche le processus, dans le cas d'un certificat de niveau de confiance de base;

b) dans la journée qui suit la date de la réception de l'information utile qui enclenche le processus, dans le cas d'un certificat de niveau de confiance moyen ou, si la réception survient un jour non ouvrable, le jour ouvrable suivant;

c) dès la réception de l'information qui enclenche le processus, dans le cas d'un certificat de niveau de confiance élevé.

SECTION 7. Rectification du certificat d'un abonné

§1. Personnes pouvant demander une rectification

115. La rectification d'un certificat peut être demandée par l'abonné ou être initiée d'office par le GCC. Toutefois, dans le cas des certificats de niveau de confiance de base, la rectification peut également être demandée par le GU lorsque le GCC le permet.

§2. Circonstances pouvant entraîner une rectification

116. La procédure de rectification peut être utilisée :

a) pour rectifier une erreur commise par le GCC lors de la création du certificat;

b) pour modifier une information inscrite dans le certificat autre que le nom de l'abonné ou qu'un renseignement que l'AVI a le devoir de vérifier selon les articles 50 à 53.

§3. Traitement d'une demande de rectification

117. Lorsque la demande provient d'un abonné ou d'un GU, le GCC doit :

a) vérifier l'identité du demandeur de manière non équivoque;

b) s'assurer que la rectification est permise selon les exigences de la présente directive.

118. Afin de rectifier un certificat, le GCC doit :

a) créer de nouveaux certificats comportant les informations mises à jour;

b) délivrer ces nouveaux certificats à l'abonné selon un protocole d'échange conforme aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale;

c) annuler les anciens certificats erronés;

d) aviser l'abonné de la rectification.

119. Le GCC doit, dans le cadre de ses responsabilités, colliger et conserver tout document relatif au traitement d'une demande de rectification ainsi que toute action subséquente posée au regard d'une telle demande. Il doit également signer tout document en attestant la réalisation et en conserver copie.

§4. Délai de traitement d'une demande de rectification

120. Le GCC doit commencer le traitement de toute demande de rectification d'un certificat dans le délai suivant :

a) dans les deux jours ouvrables qui suivent la date de la réception de la demande, dans le cas d'un certificat de niveau de confiance de base;

b) dans le délai d'un jour ouvrable qui suit la date de la réception de la demande, dans le cas d'un certificat de niveau de confiance moyen;

c) dès la réception de la demande, dans le cas d'un certificat de niveau de confiance élevé.

SECTION 8. Réattribution à la suite de l'annulation ou de l'expiration d'un certificat

§1. Personne pouvant demander une réattribution

121. Seul un abonné peut demander la réattribution de ses clés et certificats.

§2. Traitement d'une demande de réattribution

122. Le GCC doit traiter la demande de réattribution de la même manière qu'une demande de délivrance initiale, à l'exception de la vérification de l'identité qui peut être effectuée selon la procédure prévue à l'article 72.

123. Le GCC doit, dans le cadre de ses responsabilités, colliger et conserver tout document relatif au traitement d'une demande de réattribution ainsi que toute action subséquente posée au regard d'une telle demande. Il doit également signer tout document en attestant la réalisation et en conserver copie.

SECTION 9. Publication du statut du certificat d'un abonné

124. Le GCC doit s'assurer que tous les utilisateurs peuvent obtenir l'information sur le statut des certificats qu'il délivre afin de leur permettre de déterminer, au moment d'une communication, si un certificat est annulé, suspendu ou archivé.

§1. Avis d'annulation du certificat d'un abonné

125. Le GCC doit publier des listes de certificats annulés (LCA) dans lesquelles est inscrit le numéro de série des certificats annulés.

Le GCC doit assurer la mise à jour et l'intégrité des LCA qu'il délivre.

126. Les LCA doivent être mises à jour et diffusées :

a) au moins toutes les 24 heures, dans le cas des certificats de niveau de confiance de base;

b) au moins toutes les douze (12) heures, dans le cas des certificats de niveau de confiance moyen;

c) au moins toutes les quatre (4) heures, dans le cas des certificats de niveau de confiance élevé;

d) immédiatement, lorsque la modification d'une LCA résulte de l'annulation d'un certificat.

127. Un GCC peut également publier l'annulation des certificats sur un serveur de vérification en ligne qui rend disponible l'information en direct sur le statut des certificats. Cependant, lorsqu'une telle méthode est utilisée, le GCC doit tout de même continuer à publier des LCA jusqu'à ce que l'ensemble des abonnés et utilisateurs utilisent des applications ICP qui peuvent supporter la vérification en ligne.

L'information sur le serveur de vérification en ligne doit être à jour et disponible en tout temps.

128. La publication du statut annulé d'un certificat par le GCC constitue un avis aux utilisateurs. Le certificat doit être considéré comme annulé par les utilisateurs dès la publication.

§2. Avis de suspension du certificat d'un abonné

129. Le GCC doit mettre en place des mesures permettant aux utilisateurs de déterminer, au moment d'une communication, si un certificat est suspendu.

§3. Avis d'archivage du certificat d'un abonné

130. Aucun certificat de l'ICPG n'est archivé. Le GCC n'a pas à mettre en place de mesures permettant aux utilisateurs de déterminer, au moment d'une communication, si un certificat est archivé.

SECTION 10. Annulation du certificat du GCC

131. Lorsque le certificat de vérification d'un GCC doit être annulé, celui-ci doit :

a) aviser :

i) le GEAT,

ii) tous les GCC et les prestataires de services de certification externes avec qui des ententes ont été établies,

iii) tous les AVI,

iv) tous les abonnés;

b) annuler tous les certificats de reconnaissance réciproque;

c) annuler tous les certificats des abonnés;

d) générer une nouvelle paire de clés de signature et un nouveau certificat pour l'application du GCC;

e) délivrer de nouvelles clés et des nouveaux certificats à tous les abonnés;

f) signer toutes les LCA avec la nouvelle clé de signature.

Toutefois, lorsque le certificat a été annulé pour cause de compromission de la confidentialité de la clé privée de signature, le GCC doit prendre les mesures prévues à l'article 150 avant de pouvoir générer une nouvelle paire de clés de signature et un nouveau certificat.

SECTION 11. Procédures de vérification de la sécurité informatique du GCC

§1. Configuration initiale

132. Le GCC doit, pour fins de référence, documenter et conserver l'architecture et la configuration initiales de ses systèmes.

§2. Types d'événements à consigner dans les registres de vérification

133. Le GCC doit consigner tout élément d'information concernant des événements relatifs à la sécurité du système de gestion des clés et des certificats dans des registres de vérification, dont notamment :

a) les démarrages et les arrêts du système;

b) toute tentative de créer, modifier, enlever, désactiver, activer, réactiver, interdire ou récupérer les droits et les privilèges des opérateurs du système de gestion de clés et de certificats ou des opérateurs du système d'exploitation des serveurs et des postes du GCC;

c) tout changement aux mots de passe des serveurs et aux applications sur les serveurs du GCC;

d) toute modification dans les registres de vérification;

e) toute modification aux structures des bases de données;

f) tout changement à la politique de création des certificats;

g) toute tentative d'ouverture ou de fermeture de session sur le serveurs du GCC;

h) toute tentative d'accès au réseau donnant accès au système de gestion des clés et des certificats ainsi que les connexions ou écritures au répertoire par le système de gestion des clés et des certificats;

i) toute tentative d'enregistrer des abonnés et de créer, mettre à jour, révoquer, retirer ou récupérer des clés ou des certificats des abonnés ou du GCC;

j) tout changement des paramètres de sécurité du système;

k) les accès physiques au site;

l) tout changement de configuration;

m) les relevés d'activités d'entretien du système et du site;

n) tout changement de personnel;

o) tout rapport de non-conformité et de compromission de la sécurité du système du GCC;

p) la destruction de tout support contenant des clés, des codes d'initialisation ou de tout renseignement personnel ou confidentiel;

q) toute correspondance officielle.

134. Tous les registres de vérification, en format électronique ou non, doivent contenir la date et l'heure des événements enregistrés.

§3. Fréquence de traitement des registres de vérification

135. Le GCC doit assurer le traitement de toute information consignée dans les registres de vérification afin :

a) d'en identifier la nature et ses causes probables;

b) de faire enquête sur les problèmes détectés et prendre les mesures nécessaires pour les résoudre.

136. Le traitement de toute information consignée dans les registres de vérification doit être effectué :

a) au moins une fois par deux semaines dans le cas des certificats de niveau de confiance de base;

b) au moins une fois par semaine, dans le cas des certificats de niveau de confiance moyen;

c) au moins deux fois par semaine, dans le cas des certificats de niveau de confiance élevé.

§4. Délai de conservation des registres de vérification

137. Le GCC doit conserver ses registres de vérification dans les locaux abritant l'application du GCC pendant une période minimale de trois mois. Après cette période, ils doivent être conservés dans un site secondaire conforme aux exigences formulées à l'article 148 de la présente directive.

§5. Mesures de protection des registres de vérification

138. Chaque registre de vérification doit être horodaté et protégé en tout temps de façon à en conserver la confidentialité, l'intégrité et la disponibilité.

§6. Système de collecte des événements

139. Le GCC doit définir dans ses procédures de certification le système qu'il utilise pour recueillir les données de vérification.

§7. Avis à la suite d'un événement enregistré dans un registre de vérification

140. Lorsqu'un événement est consigné par un registre de vérification, le GCC n'est pas tenu d'en informer la personne ou l'entité qui en est à l'origine.

§8. Identification et traitement des vulnérabilités

141. Le GCC doit, lors du traitement de toute information relative à un événement relié à la sécurité colligée dans un registre de vérification, prendre les mesures appropriées afin d'éliminer ou de réduire les vulnérabilités des systèmes.

SECTION 12. Copie de sécurité des données

142. Une copie à jour des données suivantes doit être conservée en tout temps :

a) la base de données du GCC dans laquelle sont sauvegardés les clés et certificats du GCC et des abonnés, l'historique des clés et des certificats et les LCA;

b) les registres de vérification lorsqu'ils sont sur support numérique;

c) les données du répertoire;

d) les disques d'installation des systèmes d'exploitation;

e) les disques d'installation de l'application du GCC;

f) les disques d'installation de l'application du répertoire.

143. Les renseignements pertinents sur les abonnés doivent être sauvegardés au minimum une fois par jour ouvrable.

144. Les registres de vérification sur support papier doivent être copiés au minimum une fois par mois.

SECTION 13. Conservation des données

§1. Délais de conservation des données

145. Les certificats de signature, les certificats de chiffrement, les clés de déchiffrement, les ententes d'abonnement, les renseignements colligés afin d'établir l'identité des abonnés ainsi

que la correspondance officielle du GCC, de l'AVI, du GU et du GEAT doivent être conservés pendant une période de dix ans.

146. Les registres de vérification présentés à l'article 133 doivent être conservés par le GCC pendant une période minimale de dix ans.

§2. Calendrier de conservation

147. Les intervenants de l'ICPG tenus au respect des dispositions de la Loi sur les archives (L.R.Q. c. A-21.1) doivent modifier leur calendrier de conservation afin d'y consigner les délais de conservation prévus par la présente directive.

§3. Lieu de conservation des données

148. Une copie de toutes les données qui doivent être conservées selon la présente directive par le GCC doit l'être dans un site secondaire et doit être protégée par des mesures de sécurité physique, ou une combinaison de mesures de sécurité physique et cryptographique. Un tel site doit offrir un environnement propice à l'emmagasinage du matériel, plus particulièrement en ce qui a trait à la température, à l'humidité et à la protection contre le magnétisme. Il doit par ailleurs répondre à des exigences de sécurité égales ou supérieures à celles relatives au centre de gestion des clés et des certificats qui sont définies à l'article 160.

SECTION 14. Compromission, corruption et désastre

§1. Corruption des équipements, des logiciels et des données

149. Le GCC doit établir des procédures visant à assurer le maintien de ses activités et décrire les étapes prévues en cas de corruption ou de pertes de ressources informatiques, de logiciels ou de données.

§2. Compromission de la confidentialité de la clé d'un GCC

150. Lorsque la confidentialité de la clé privée de signature d'un GCC est compromise, le GCC doit :

a) annuler son certificat en effectuant les opérations prescrites à l'article 131;

b) corriger les facteurs ayant mené à cette compromission;

c) fournir au GEAT la preuve de la correction et obtenir l'autorisation de générer sa nouvelle paire de clés de signature.

§3. Compromission de la confidentialité de la clé de signature d'un AVI

151. Lorsque la confidentialité de la clé privée de signature d'un AVI est compromise, l'AVI doit en informer le GEAT ainsi que tous les GCC avec qui il collabore.

152. Dans une telle situation, les GCC avec qui cet AVI collabore doivent alors annuler tout certificat ayant été délivré à un abonné à la suite de la vérification de son identité par l'AVI concerné après la date de cette compromission.

§4. Recouvrement à la suite d'un désastre

153. Le GCC doit définir dans un plan de relève les mesures à prendre pour rétablir une installation sécuritaire en cas de catastrophe naturelle ou de tout autre type de sinistre majeur.

Un tel plan doit décrire les moyens qui seront mis en place par le GCC afin que les services de gestion de clés et de certificats soient repris dans les délais suivants :

a) dans les deux jours ouvrables qui suivent la date du sinistre, dans le cas des certificats de niveau de confiance de base;

b) dans les 48 heures qui suivent le moment où est survenu le sinistre, dans le cas des certificats de niveau de confiance moyen;

c) dans les 24 heures qui suivent le moment où est survenu le sinistre, dans le cas de certificats de niveau de confiance élevé.

154. Le GCC doit effectuer des tests de reprise des services au minimum une fois par année pour les certificats de niveaux de confiance de base et moyen, et deux fois par année pour le niveau de confiance élevé.

SECTION 15. Cessation des activités

§1. Cessation des activités d'un GCC

155. La cessation des activités d'un GCC doit être effectuée selon des modalités approuvées par le GEAT.

156. Un GCC doit, dans un délai raisonnable, informer préalablement ses abonnés de la cessation de ses activités et prendre des dispositions pour transférer ses dossiers et ses données à un autre GCC désigné par le GEAT.

157. Lorsque requis, les certificats délivrés par le GCC qui cesse ses activités peuvent être annulés.

§2. Cessation des activités d'un AVI

158. Un AVI doit, dans un délai raisonnable, informer préalablement le GEAT et les GCC avec qui il collabore de la cessation de ses activités et prendre des dispositions pour faciliter le transfert de ses dossiers selon les modalités définies par le GEAT.

159. Lorsque nécessaire, les certificats de l'AVI qui cesse ses activités peuvent être annulés.

CHAPITRE 4. Mesures de sécurité physique, administrative et du personnel

SECTION 1. Mesures de sécurité physique

§1. Mesures de sécurité physique pour le centre de gestion des clés et des certificats

160. Le centre de gestion des clés et des certificats doit être localisé dans une zone de sécurité conforme aux normes minimales suivantes :

a) les murs de la zone de sécurité doivent être renforcés allant du vrai plancher au vrai plafond ou au plafond suspendu avec système de détection d'intrusion par le plafond suspendu;

b) le cas échéant, les fenêtres et les ouvertures de service de la zone de sécurité doivent être obstruées par un grillage ou par un laminé anti-intrusion, ne permettant pas de voir les écrans d'ordinateur à l'intérieur du local;

c) la porte de la zone de sécurité doit être munie d'un verrou de sécurité;

d) l'accès à la zone de sécurité ne doit être possible qu'à partir d'une autre zone à accès contrôlé et non depuis une zone à accès public;

e) la zone de sécurité doit être pourvue d'un système de surveillance ou, lorsque la surveillance n'est pas possible, d'un système de détection d'intrusion actif en l'absence d'une personne autorisée;

f) la zone de sécurité doit être pourvue d'un panneau d'identification limitant l'accès au personnel autorisé seulement, affiché en évidence près des portes d'accès;

g) la zone de sécurité doit être dotée d'une alimentation électrique d'appoint conforme aux normes de protection contre le feu du gouvernement du Québec;

h) la climatisation de la zone de sécurité doit être suffisante aux besoins des ordinateurs s'y trouvant et conforme aux normes de protection contre le feu du gouvernement du Québec;

i) la zone de sécurité doit être pourvue d'une procédure documentée de destruction des documents confidentiels et des supports contenant de tels documents.

De plus, le GCC doit prendre les mesures nécessaires afin de :

a) s'assurer que l'accès au système du GCC est limité aux seules personnes autorisées par lui;

b) s'assurer que toute personne qui n'est pas un employé autorisé du GCC et qui doit avoir accès au système soit accompagnée et surveillée par une personne autorisée;

c) s'assurer qu'un journal des accès au centre de gestion des clés et des certificats est tenu et vérifié périodiquement;

d) s'assurer que tous les supports amovibles et documents sur support papier contenant de l'information délicate en clair soient entreposés de manière à ce que seuls les membres autorisés y aient accès;

e) établir des procédures de conservation, de transfert et de destruction des renseignements confidentiels sur supports magnétique et papier.

§2. Mesures de sécurité physique pour le répertoire

161. Le répertoire doit, selon le cas :

a) faire l'objet de mesures de sécurité physique similaires à celles généralement en vigueur pour les serveurs gouvernementaux de fichiers ou de données de nature confidentielle, dans le cas des certificats de niveaux de confiance de base ou moyen;

b) faire l'objet de mesures de sécurité physique équivalentes à celles du centre de gestion des clés et des certificats, dans le cas des certificats de niveau de confiance élevé.

§3. Mesures de sécurité physique pour l'AVI

162. L'AVI doit prendre toutes les mesures nécessaires pour protéger l'information confidentielle recueillie lors de la vérification d'identité. Lorsque cette information est emmagasinée sur son poste de travail, elle doit être protégée par le chiffrement des données.

L'AVI doit empêcher l'accès à son poste de travail lorsque ses clés privées sont accessibles.

163. Pour les certificats de niveau de confiance élevé, l'AVI doit exercer ses fonctions dans un site sécurisé répondant aux exigences du GEAT. Notamment, des mesures de sécurité particulières sont requises lorsque l'AVI utilise un logiciel spécialisé, surtout si des renseignements confidentiels sont échangés en ligne avec l'application du GCC, par exemple les codes d'initialisation.

§4. Mesures de sécurité physique pour les abonnés

164. L'abonné doit prendre les mesures nécessaires afin d'assurer la sécurité et la confidentialité de ses clés privées.

À cette fin, il ne doit pas quitter son poste de travail lorsque ses clés sont activées, à moins que celles-ci aient été affectées à une application ou à un dispositif.

L'abonné détenteur d'un certificat de niveau de confiance élevé doit conserver ses clés privées sur un support matériel qui doit demeurer en sa possession en tout temps.

§5. Alimentation électrique et climatisation

165. L'alimentation électrique et la climatisation du centre de gestion des clés et des certificats doivent être conformes aux spécifications techniques relatives aux équipements s'y trouvant.

§6. Risques reliés aux dégâts d'eau

166. Le GCC doit prendre les mesures nécessaires pour que son système soit protégé contre les dégâts causés par l'eau.

§7. Protection et prévention des incendies

167. Le centre de gestion des clés et des certificats doit être équipé d'un système de détection et de suppression des incendies.

§8. Conservation des supports magnétiques et physiques

168. Tous les supports magnétiques et physiques doivent être protégés adéquatement contre les menaces environnementales (température, humidité, magnétisme).

§9. Destruction des supports

169. Tous les supports servant au stockage de l'information doivent être soit nettoyés de manière à ce que les informations ne puissent être récupérées, soit détruits de façon permanente avant d'être mis au rebut.

SECTION 2. Mesures de sécurité administrative et opérationnelle

§1. Structure organisationnelle du centre de gestion

170. Le GCC doit, afin de se prémunir contre toute personne qui, agissant seule, pourrait porter préjudice à la sécurité et à l'intégrité des services de certification, s'assurer que les fonctions liées à des tâches essentielles soient réparties entre plusieurs personnes. Le GCC doit au minimum faire en sorte que les fonctions opérationnelles soient assumées par des membres de son personnel qui soient différents de ceux assumant les fonctions de vérification. Une même personne ne peut en aucun cas occuper ces deux rôles au même moment.

§2. Nombre de personnes requises pour effectuer les tâches

171. Au moins deux personnes faisant partie du personnel du GCC doivent collaborer pour effectuer les tâches suivantes :

a) déterminer et modifier la période de validité des clés;

b) déterminer et modifier la période de validité des LCA;

c) créer et modifier les identificateurs d'objet;

d) faire toute opération relative à l'attribution de droits et de privilèges au personnel du GCC;

e) mettre à jour la clé privée de signature du GCC.

§3. Vérification des autorisations du personnel

172. Les autorisations relatives à un membre du personnel devant occuper un poste relié à la gestion des clés et des certificats doivent être vérifiées avant :

a) qu'il soit autorisé à accéder au centre de gestion des clés et des certificats;

b) qu'il obtienne un compte d'usager du système d'exploitation et de l'application du GCC.

173. Les comptes doivent être directement attribuables à l'individu et les droits et privilèges limités à ceux requis pour que l'individu effectue ses tâches.

174. Toute personne qui accède au système de gestion de clés et de certificats par l'intermédiaire de réseaux partagés doit être identifiée à l'aide d'un jeton matériel et de processus cryptographiques.

SECTION 3. Mesures de sécurité du personnel du GCC

§1. Profil du personnel du GCC

175. Les personnes impliquées dans la gestion des clés et des certificats doivent :

a) avoir reçu la formation nécessaire pour accomplir leurs tâches;

b) n'effectuer aucune autre tâche qui risque de les placer en situation de conflit d'intérêts avec les tâches qui leur incombent à l'égard du GCC;

c) respecter le Règlement sur les normes d'éthique, de discipline et le relevé provisoire des fonctions dans la fonction publique (R.R.Q. F-3.1.1, r.1 et ses modifications) ou, si elles ne sont pas visées par ce règlement, être soumises par contrat ou une autre loi à des obligations équivalentes.

§2. Formation

176. Le GCC doit s'assurer que les compétences professionnelles des personnes qu'il emploie correspondent aux tâches qui leur sont confiées.

177. Les membres du personnel du GCC doivent suivre un programme de formation spécifique à leurs fonctions et couvrant notamment les sujets suivants dans la mesure où ils les concernent :

a) les mesures de sécurité en vigueur;

b) l'application du GCC et toutes autres applications devant être utilisées par le personnel;

c) la présente directive et les Spécifications techniques pour l'infrastructure à clés publiques gouvernementale ;

d) les procédures de certification et les procédures opérationnelles;

e) les procédures de contingence et de recouvrement des opérations.

§3. Formation continue

178. Le GCC doit revoir son programme de formation sur une base annuelle afin de le maintenir à jour. Les membres du personnel du GCC doivent prendre des cours de rappel ou de mise à niveau lorsque requis.

§4. Sanctions à la suite d'actes non autorisés ou négligents

179. Lorsque le GCC a des motifs raisonnables de douter de la fiabilité ou de la compétence d'un membre de son personnel, il doit immédiatement lui interdire l'accès à l'application du GCC.

§5. Personnel contractuel

180. Les mesures de sécurité du personnel spécifiées à la présente section sont les mêmes quel que soit le lien avec le GCC.

§6. Documentation fournie au personnel

181. Le GCC doit mettre à la disposition des membres de son personnel la présente directive, les procédures de certification ainsi que toute procédure opérationnelle ou autre documentation se rattachant à leurs fonctions.

SECTION 4. Mesures de sécurité relatives aux AVI

182. L'AVI doit :

a) avoir reçu la formation prescrite pour accomplir ses tâches;

b) n'effectuer aucune autre tâche qui risque de le placer en situation de conflit d'intérêts avec les tâches qui lui incombent en vertu de la présente directive;

c) respecter le Règlement sur les normes d'éthique, de discipline et le relevé provisoire des fonctions dans la fonction publique ou, s'il n'est pas visé par ce règlement, être soumis par contrat ou une autre loi à des obligations équivalentes.

CHAPITRE 5. Mesures de sécurité technique

SECTION 1. Génération et livraison des clés et des certificats

§1. Génération de paires de clés

183. L'application du GCC doit supporter la gestion de deux paires de clés distinctes, l'une servant au chiffrement et l'autre à la signature. Les paires de clés doivent être générées à l'aide d'algorithmes cryptographiques conformes aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

184. Pour les certificats de niveau de confiance de base, les clés de signature peuvent être générées sur le poste de travail de l'abonné ou par le GCC.

Pour les certificats de niveau de confiance moyen, les clés de signature doivent être générées par l'abonné sur un poste de travail dont il a le contrôle.

Pour les certificats de niveau de confiance élevé, les clés de signature doivent être générées sur un jeton cryptographique dans les locaux sécurisés de l'AVI.

§2. Livraison des clés privées

185. La clé privée de déchiffrement doit être livrée à l'abonné selon un protocole d'échange sécurisé conforme aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

186. Pour les certificats de niveau de confiance de base, la clé privée de signature peut être générée par le GCC, auquel cas elle doit être livrée à l'abonné selon un protocole d'échange sécurisé conforme aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

§3. Livraison des clés publiques

187. Les clés publiques doivent être livrées à l'application du GCC selon un protocole d'échange sécurisé conforme aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

§4. Livraison de la clé publique de vérification du GCC à l'abonné

188. La clé publique de vérification de signature de l'application du GCC doit être livrée à l'abonné selon un protocole d'échange sécurisé conforme aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

§5. Longueur et période de validité des clés

189. La longueur des clés et leur période de validité doivent être conformes aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

§6. Génération matérielle et logicielle des clés

190. Pour les certificats de niveaux de confiance de base et moyen, la paire de clés du GCC et de toute autre entité peut être générée par un module cryptographique logiciel ou matériel.

191. Pour les certificats de niveau de confiance élevé, toutes les paires de clés doivent être générées par un module cryptographique matériel.

§7. Utilisation du champ d'extension « utilisation de la clé » (key usage)

192. Le champ d'extension « utilisation de la clé » (*key usage*) des certificats des abonnés et du certificat de vérification de l'application du GCC doit être utilisé conformément aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

§8. Génération des certificats de l'abonné

193. Les certificats des abonnés doivent être générés par l'application du GCC, lequel garantit leur intégrité en y apposant sa signature.

SECTION 2. Protection des clés privées du GCC

§1. Clé privée de signature du GCC

194. L'intervention conjointe de deux personnes autorisées est requise pour les opérations relatives à la clé privée de l'application du GCC.

§2. Clés du personnel du GCC

195. Lorsqu'un membre du personnel du GCC utilise des clés privées pour s'authentifier auprès de l'application du GCC à partir d'un réseau partagé ou d'un réseau public, ces clés doivent être conservées sur un support cryptographique matériel et demeurer en permanence sous le contrôle de leur détenteur.

SECTION 3. Protection des clés privées de l'abonné

§1. Conservation et support des clés

196. Les clés privées de l'abonné doivent être conservées dans un environnement personnel sécurisé (EPS). Cet environnement personnel sécurisé doit permettre d'assurer l'intégrité des clés et doit comporter des mesures de contrôle d'accès aux clés suffisamment robustes pour préserver leur confidentialité. Cet environnement personnel sécurisé doit également répondre aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

197. Pour les niveaux de confiance de base et moyen, la clé privée de signature doit être conservée sur un support logiciel (disque dur, etc.). L'abonné peut conserver une copie de ses clés privées pour fins de sauvegarde. L'abonné doit prendre les mesures nécessaires afin d'assurer la sécurité et la confidentialité de cette copie.

198. Pour le niveau de confiance élevé, la clé privée de signature doit être conservée sur un jeton cryptographique matériel (une carte à puce, par exemple).

§2. Conservation par un tiers

199. Une copie des clés privées de déchiffrement doit être conservée par le GCC en prévision d'une éventuelle récupération. Ces clés doivent être chiffrées en tout temps.

§3. Transfert de la clé privée dans le module cryptographique

200. Si une clé privée n'est pas générée dans le module cryptographique de l'abonné, elle doit y être transférée selon un protocole d'échange sécurisé conforme aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

§4. Méthode d'activation

201. Par mesure de sécurité, l'accès aux clés privées d'un abonné doit être protégé par un mot de passe ou une autre donnée unique appelée « donnée d'activation ». L'abonné doit entrer sa donnée d'activation pour activer ses clés avant d'effectuer des opérations cryptographiques, notamment signer ou déchiffrer des documents.

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

a) elle doit comporter un minimum de huit caractères;

b) elle doit être constituée d'une combinaison de lettres majuscules, de lettres minuscules et de chiffres;

c) elle ne doit pas contenir plus de quatre fois le même caractère.

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

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

§5. Méthode de désactivation

204. La désactivation des clés privées consiste à rendre les clés de l'abonné inactives et chiffrées. Cette mesure de sécurité fait en sorte qu'une personne autre que l'abonné ne pourrait utiliser les clés à moins d'avoir en sa possession la donnée d'activation qui permet d'y accéder, par exemple le mot de passe choisi par l'abonné.

L'application de l'abonné doit faire en sorte que les clés privées soient désactivées automatiquement après une période d'inactivité définie au préalable, mais ne pouvant dépasser 10 minutes. De même, avant de quitter son poste de travail, l'abonné doit toujours vérifier que ses clés privées sont désactivées.

§6. Méthode de destruction

205. Lorsqu'un abonné n'utilise plus ses clés privées, il doit détruire le fichier de clés privées de manière à ce que les données soient irrécupérables. Lorsque les clés sont conservées sur un jeton cryptographique, l'abonné doit, selon le cas, soit le réinitialiser, soit le remettre à l'AVI,

au GU ou au GCC, lequel doit alors le détruire ou le réinitialiser de manière à en effacer définitivement le contenu.

SECTION 4. Mesures de sécurité des ordinateurs

§1. Mesures de sécurité pour le GCC

206. Le GCC doit utiliser une application de gestion des clés et des certificats conforme aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

207. Le système utilisé pour effectuer la gestion des clés et des certificats doit être protégé par les mesures de sécurité suivantes :

a) être pourvu d'un contrôle de l'accès aux services et aux rôles définis dans l'application du GCC;

b) prévoir la séparation des tâches selon les rôles définis;

c) permettre l'identification et la vérification de l'identité;

d) prévoir un processus de réinitialisation de la mémoire vive et du disque rigide pour les régions retournées au système d'exploitation;

e) permettre l'utilisation du chiffrement pour les sessions de communication et la sécurisation des bases de données;

f) permettre l'enregistrement et la conservation des événements relatifs à la sécurité;

g) procéder à la vérification automatique des mécanismes de sécurité;

h) comporter un chemin de confiance pour l'identification et la vérification de l'identité;

i) comporter un mécanisme de reprise;

j) procurer l'assurance de la robustesse des mécanismes empêchant qu'un processus informatique relatif à la sécurité puisse être affecté ou corrompu par un autre processus informatique.

Ces mesures peuvent être des fonctions du système d'exploitation ou de l'application du GCC.

208. Le GCC doit s'assurer de la mise en place d'un système de gestion de la configuration pour l'application du GCC, les systèmes d'exploitation, les composantes réseau et tout autre système supportant l'application du GCC.

§2. Mesures de sécurité pour l'AVI

209. Le poste de travail d'un AVI doit comporter des mesures de sécurité permettant de préserver la confidentialité et l'intégrité des données concernant les abonnés, y compris lors de la communication de ces données.

210. Pour les certificats de niveau de confiance élevé, le poste de travail de l'AVI doit être conforme aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

SECTION 5. Mesures de sécurité des réseaux

211. L'application du GCC doit être protégée des attaques pouvant venir d'un réseau auquel elle est branchée. Cette protection peut venir d'une composante matérielle ou logicielle permettant uniquement les commandes et les protocoles requis pour le bon fonctionnement de cette application.

212. L'interconnexion avec des réseaux publics doit être protégée par des bastions et un système d'exploitation configurés pour n'accepter que les protocoles applicables à la gestion des clés et des certificats.

SECTION 6. Mesures de contrôle d'ingénierie des modules cryptographiques

213. Les modules servant à la génération des clés ainsi qu'aux opérations cryptographiques doivent être conformes aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

CHAPITRE 6. Format et contenu des certificats, des LCA et des répertoires

SECTION 1. Format et contenu des certificats

§1. Format des certificats

214. Le GCC doit délivrer des certificats dans un format conforme aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

§2. Contenu des certificats

215. Un certificat doit comprendre les renseignements suivants :

a) le nom distinctif du GCC qui a délivré le certificat ainsi que sa signature;

b) l'identificateur d'objet faisant référence à la présente directive et indiquant le type de certificat selon l'article 29;

c) la version de certificat et le numéro de série du certificat;

d) le début et la fin de la période de validité du certificat;

e) le nom distinctif de l'abonné, lequel peut, le cas échéant, être remplacé par celui du groupe, du rôle, du dispositif ou de l'application auquel l'abonné a affecté le certificat;

f) le cas échéant, l'identification ou l'acronyme d'un ministère, d'un organisme public, d'une personne morale, d'une société ou d'une association.

Un certificat peut également comporter, de manière facultative, l'adresse de courrier électronique de l'abonné ainsi que l'identification d'une unité administrative gouvernementale.

§3. Formulation du nom distinctif

216. Chaque certificat doit contenir un nom distinctif dans un format conforme aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

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

Le certificat peut également contenir l'identification ou l'acronyme du ministère, de l'organisme public, ou de toute autre personne morale, société ou association représentée par l'abonné.

Lorsqu'un certificat est délivré à un abonné pour un groupe, un rôle, un dispositif ou une application, le nom de l'abonné peut être remplacé par l'identification du groupe, du rôle, du dispositif ou de l'application auquel l'abonné désire affecter son certificat. Le certificat ainsi affecté doit également comporter l'identification ou l'acronyme du ministère, de l'organisme public, de la personne morale, de la société ou de l'association visé.

218. Les noms distinctifs doivent être uniques pour tous les certificats délivrés par un GCC. Il appartient à ce dernier de s'en assurer.

§4. Inscription de renseignements au certificat

219. L'inscription de renseignements au certificat doit être effectuée selon les circonstances, par les personnes et selon les procédures prévues dans la présente directive pour la délivrance initiale, la rectification ou la réattribution de certificats.

220. Seul l'abonné peut demander au GCC l'inscription d'un renseignement au certificat.

§5. Interprétation et traitement des certificats

221. Les applications ICP doivent interpréter et traiter correctement tous les renseignements contenus dans les certificats.

SECTION 2. Format et contenu des listes de certificats annulés

222. Le GCC doit délivrer des listes de certificats annulés conformes aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale. Les LCA doivent contenir les renseignements suivants :

a) le nom distinctif du GCC qui a délivré la LCA;

b) la date et l'heure de délivrance de la LCA;

c) la date et l'heure de délivrance de la prochaine LCA;

d) le numéro de série des certificats annulés;

e) la signature du GCC.

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

SECTION 3. Format et contenu du répertoire

224. Le format du répertoire doit être conforme aux Spécifications techniques pour l'infrastructure à clés publiques gouvernementale.

225. Pour les fins de l'ICPG, le répertoire ne doit contenir que les certificats de chiffrement des abonnés et les LCA. Aucune personne autre que le GCC ne peut inscrire ou faire inscrire des renseignements au répertoire. Cependant, l'abonné peut demander au GCC la modification ou la suppression d'un renseignement le concernant.

SECTION 4. Périodicité et procédure de mise à jour des certificats, des LCA et du répertoire

226. Toute opération subséquente sur les certificats déclenche, s'il y a lieu, la mise à jour des certificats et du contenu du répertoire.

De plus, les LCA inscrites au répertoire sont mises à jour et publiées périodiquement selon les modalités indiquées à l'article 126.

CHAPITRE 7. Administration de la directive

SECTION 1. Procédure de désignation des intervenants de l'ICPG

§1. Gestionnaire des clés et des certificats

227. La personne ou l'organisation qui demande au GEAT d'être désignée comme GCC doit démontrer que ses procédures de certification sont conformes aux exigences de la présente directive. Ces procédures doivent comporter la description des services de certification offerts ainsi que la description des mesures de sécurité mises en place pour assurer la disponibilité et l'intégrité des services.

§2. Gestionnaire de l'utilisation

228. Un ministère ou un organisme public visé à l'article 3 devient un GU de l'ICPG dès lors qu'il a conclu une entente de service avec un GCC désigné visant l'utilisation de clés et de certificats.

§3. Agent de vérification de l'identité

229. Le GEAT désigne les personnes ou les catégories de personnes habilitées à agir comme AVI au sein de l'ICPG et détermine leur domaine d'activité.

230. Une personne désignée par le GEAT qui désire agir comme AVI doit se conformer en tout temps aux exigences du GEAT, notamment réussir le programme de formation approuvé par le GEAT.

§4. Gestionnaire de l'infrastructure opérationnelle

231. La personne ou l'organisation qui demande au GEAT d'être désignée comme GIO doit démontrer que ses procédures de gestion sont conformes aux exigences de la présente directive. Ces procédures doivent comporter la description des services de gestion offerts ainsi que la description des mesures de sécurité mises en place pour assurer la disponibilité et l'intégrité des services du ou des GCC qu'il sert.

232. Un GIO dûment désigné ne peut exécuter que les fonctions dont le GEAT a autorisé la délégation au moment de la désignation.

§5. Perte de la désignation

233. Lorsqu'un intervenant de l'ICPG ne respecte plus ses obligations en vertu de la présente directive ou ne remplit plus les conditions en vertu desquelles il a été désigné, le GEAT peut prendre toute mesure qu'il juge appropriée, notamment lui retirer la désignation dont il bénéficie.

SECTION 2. Vérification de conformité

§1. Vérification préalable à la désignation

234. Le GEAT peut exiger d'un GCC ou d'un GIO, préalablement à sa désignation, un rapport de conformité de ses activités aux exigences de la présente directive. La vérification de conformité doit être effectuée par une firme externe et indépendante approuvée par le GEAT.

§2. Vérification annuelle

235. Le GEAT peut exiger annuellement d'un GCC ou d'un GIO, sur avis préalable de trois mois, un rapport de conformité de ses activités aux exigences de la présente directive. Cette vérification de conformité doit être effectuée par une firme externe et indépendante approuvée par le GEAT.

§3. Vérification ponctuelle

236. Lorsque le niveau de confiance des services de l'ICPG est mis en cause, le GEAT peut exiger du GCC, du GIO, du GU ou de l'AVI qu'il produise un rapport de conformité de ses activités aux exigences de la présente directive. Cette vérification de conformité est effectuée suivant les modalités définies par le GEAT.

§4. Conséquences de la vérification

237. À la suite d'une vérification de conformité, le GEAT peut prendre toute mesure qu'il juge appropriée, notamment :

a) Signaler les irrégularités, mais permettre à l'intervenant de l'ICPG de continuer ses activités jusqu'à la prochaine vérification;

b) révoquer le certificat de l'intervenant de l'ICPG, le cas échéant;

c) modifier ou retirer la désignation de l'intervenant de l'ICPG.

SECTION 3. Procédures de modifications de la directive

§1. Comité consultatif

238. Aux fins de consultation relativement à des modifications à la présente directive, le GEAT doit soumettre tout projet de modification à un comité constitué d'un représentant de chacun des GCC désignés, de chacun des GIO désignés, de chacune des catégories d'AVI désignés et de toute autre personne dont l'expertise et les compétences pourraient être nécessaires. Le GEAT assure la présidence et le secrétariat de ce comité.

§2. Modifications qui requièrent un nouvel identificateur d'objet

239. Si, selon l'évaluation du comité, des modifications à la directive ont une incidence majeure sur un nombre important d'abonnés ou d'utilisateurs, le GEAT doit créer un nouveau type de certificat et produire un nouvel identificateur d'objet.

§3. Modifications qui requièrent un avis

240. Toute modification qui, de l'avis du GEAT, a une incidence majeure sur un intervenant de l'ICPG doit faire l'objet d'un avis.

241. Le GEAT avise par courrier électronique ou régulier les GCC, les GIO et les GU des modifications proposées. L'avis doit contenir la liste des modifications proposées, la date à laquelle prend fin la collecte des commentaires, le cas échéant, et la date à laquelle les modifications seront en vigueur.

Selon la nature des modifications, le GEAT peut demander au GCC d'aviser ses abonnés et ses utilisateurs des modifications proposées.

§4. Version de la directive

242. Le GEAT doit mettre en place des procédures permettant de déterminer en tout temps quelle version de la directive est en vigueur. Le GEAT doit également fournir à toute personne qui en fait la demande les versions antérieures de la directive.

SECTION 4. Publication de la directive

243. La présente directive est accessible sur le site Web du Secrétariat du Conseil du trésor. Le GCC doit également rendre accessible en ligne cette directive aux abonnés et aux utilisateurs.

Le Secrétariat du Conseil du trésor publie sur son site Web toute autre information additionnelle qui doit être portée à la connaissance des abonnés et des utilisateurs, notamment en ce qui a trait à la mise à jour des limites à l'utilisation des clés et des certificats, le cas échéant.

SECTION 5. Spécifications techniques pour l'infrastructure à clés publiques gouvernementale

244. Le GEAT doit élaborer les Spécifications techniques pour l'infrastructure à clés publiques gouvernementale en conformité avec les exigences de la Loi concernant le cadre juridique des technologies de l'information.

245. Avant de déterminer ces spécifications techniques, le GEAT doit en soumettre un projet au comité consultatif prévu à l'article 238. Le GEAT doit également soumettre au comité tout projet de modification de ces spécifications.

246. Les Spécifications techniques pour l'infrastructure à clés publiques gouvernementale sont accessibles sur le site Web du Secrétariat du Conseil du trésor. Le GCC doit également les rendre accessibles en ligne aux abonnés et aux utilisateurs.

CHAPITRE 8. Dispositions diverses

SECTION 1. Protection des renseignements personnels

247. Tous les renseignements recueillis, utilisés, conservés ou communiqués par le GEAT, les GCC, les GIO, les GU et les AVI sont assujettis, selon le cas, à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ou à la Loi sur la protection des renseignements personnels dans le secteur privé (L.R.Q, c. P-39.1). Notamment, toutes les informations recueillies dans le cadre de la délivrance, de l'utilisation ou de la gestion des clés et des certificats ne doivent être utilisées ou communiquées que pour les fins pour lesquelles elles ont été recueillies.

248. En aucune circonstance un GCC ou un GIO ne peut recueillir d'information relative aux habitudes d'utilisation des clés et des certificats des abonnés et des utilisateurs. À cet égard, le GCC ou le GIO ne peut dresser aucun profil ou n'effectuer aucune analyse de comportement d'un abonné et d'un utilisateur à partir d'une information recueillie dans le cadre de la gestion des clés et des certificats.

SECTION 2. Mécanismes de traitement des plaintes

249. Tout abonné ou tout utilisateur peut déposer une plainte concernant les services de certification offerts dans le cadre de l'ICPG en s'adressant à un GU. Lorsque le GU est dans l'impossibilité de traiter la plainte à la satisfaction de cet abonné ou de cet utilisateur, il doit la transmettre au GCC ou à l'AVI concerné, selon l'objet de la plainte.

250. Tout intervenant de l'ICPG, autre qu'un abonné ou un utilisateur, qui reçoit une plainte doit la traiter dans les meilleurs délais et en documenter le traitement.

SECTION 3. Règlement des litiges entre les intervenants de l'ICPG

251. Tout conflit entre les intervenants de l'ICPG peut être soumis au GEAT et réglé suivant la procédure déterminée par ce dernier.

SECTION 4. Renseignements dont l'exactitude est confirmée

§1. Renseignements inscrits au certificat

252. Le prestataire de services de certification confirme l'exactitude des informations dont l'inscription au certificat est obligatoire selon l'article 215.

Toutefois, le prestataire de services de certification ne confirme aucunement l'exactitude de tout autre renseignement inscrit au certificat, tel l'adresse de courrier électronique ou le nom des unités administratives gouvernementales.

§2. Renseignements inscrits au répertoire

253. Le prestataire de services de répertoire confirme l'exactitude des LCA inscrites au répertoire.

SECTION 5. Garanties

254. Le prestataire de services de certification et de répertoire garantit qu'il a pris les moyens raisonnables pour s'assurer que les renseignements dont il confirme l'exactitude en vertu des articles 252 et 253 sont exacts.

Toutefois, cette garantie ne s'étend pas à l'exactitude de tout autre renseignement pouvant être inscrit dans un certificat ou dans un répertoire.

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

SECTION 6. Entente d'abonnement à l'ICPG

256. L'entente d'abonnement à l'ICPG doit, au minimum :

a) rappeler à l'abonné ses obligations relativement à l'utilisation de ses clés et de ses certificats, dont celle de préserver la confidentialité de sa donnée d'activation ainsi que celle d'aviser le GCC lorsqu'il constate ou qu'il soupçonne que la confidentialité de ses clés privées a été compromise;

b) obtenir de l'abonné, en contrepartie de son droit à l'utilisation des services de l'ICPG, son consentement à la collecte, à l'utilisation et, le cas échéant, à la communication de renseignements personnels qui le concernent, dans le respect des lois applicables en matière de protection des renseignements personnels.

257. Le prestataire de services de certification peut mettre fin en tout temps à l'entente d'abonnement d'un abonné moyennant un avis préalable de 15 jours.

CHAPITRE 9. Dispositions transitoires et finales

SECTION 1. Dispositions transitoires

§1. Secret partagé

258. Malgré les dispositions de l'article 62, un secret partagé transmis au GCC par l'AVI peut être utilisé dans les deux années qui suivent la date d'entrée en vigueur de la présente directive, lorsque les deux premières conditions énumérées sont remplies.

§2. Numéro d'identificateur d'objet

259. Malgré les dispositions des articles 29 et 215, tout certificat délivré par un GCC, dans l'année qui suit la date d'entrée en vigueur de la présente directive, et portant le numéro d'identificateur d'objet 2.16.124.10.101.8.5.1.1.1.20, est assimilé à un certificat délivré en vertu de la présente directive sous le numéro d'identificateur d'objet 2.16.124.10.101.8.5.3.1.1.20 et tout certificat ainsi délivré est réputé conférer les mêmes droits et les mêmes obligations que ceux établis en faveur d'un certificat délivré sous l'autorité de la présente directive.

De même, tout certificat délivré par un GCC et portant le numéro d'identificateur d'objet 2.16.124.10.101.8.5.1.1.2.20 est assimilé à un certificat délivré en vertu de la présente directive sous le numéro d'identificateur d'objet 2.16.124.10.101.8.5.3.1.2.20 et tout certificat ainsi délivré est réputé conférer les mêmes droits et les mêmes obligations que ceux établis en faveur d'un certificat délivré sous l'autorité de la présente directive.

§3. Évaluation des procédures de certification du GCC

260. Malgré les dispositions de l'article 227, le GEAT n'est pas tenu de vérifier la conformité des procédures de certification des GCC qui, au moment de l'entrée en vigueur de la présente directive, avaient déjà été désignés en qualité de gestionnaire de clés et de certificats par le Conseil du trésor. Cependant, le GEAT peut exiger de ces GCC qu'ils produisent, à l'expiration du délai de six mois suivant la date de l'entrée en vigueur de la présente directive, le rapport de conformité prévu à l'article 234.

SECTION 2. Disposition finale

261. La présente directive entre en vigueur le 13 février 2002.