Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC au sein des entreprises du secteur privé canadien

ITSD-06A

Canada

Avant-propos

La *Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC au sein des entreprises du secteur privé canadien* (ITSD-06A) est un document NON CLASSIFIÉ publié avec l'autorisation du chef du Centre de la sécurité des télécommunications, conformément à la *Politique sur la sécurité du gouvernement* du Secrétariat du Conseil du Trésor du Canada.

La présente publication remplace la *Directive sur le contrôle du matériel COMSEC dans le secteur privé canadien* (ITSD-06) datant de juin 2013, ainsi que toutes les versions antérieures, lesquelles doivent être détruites conformément aux procédures ministérielles en matière de disposition de l'information non classifiée.

Les demandes de renseignements généraux et les suggestions de modifications doivent être transmises aux Services à la clientèle en matière de COMSEC du Centre de la sécurité des télécommunications, par l'entremise des responsables de la sécurité des communications du ministère (voir la section 1.12).

Le Centre de la sécurité des télécommunications informera les utilisateurs des changements apportés à la présente publication.

Date d'entrée en vigueur

La présente directive entre en vigueur au moment de sa signature.

Exemplaire original signé **le 15 juin 2016**
par Joe Waddington, directeur général, Cyberprotection,
au nom du chef adjoint de la sécurité des TI

Reproduction et diffusion

Résumé des modifications apportées à l'ITSD-06 aux fins de la présente ITSD

Référence	Modification
Ancienne annexe B	L'annexe B sur le contrôle du matériel COMSEC en cours de réalisation a été retirée et intégrée à une nouvelle directive distincte (c.-à-d. l'ITSD-08).
Ancienne annexe D	Les instructions sur la façon de remplir le *Rapport de matériel COMSEC* (GC-223) ont été retirées et se trouvent désormais à l'adresse suivante : https://www.cse-cst.gc.ca/fr/group-groupe/high-assurance-technologies.
Ancienne annexe E	La façon de remplir le nouveau *Registre de contrôle du matériel COMSEC* est suffisamment explicite. Les anciennes instructions ont donc été retirées, et le formulaire se trouve désormais à l'adresse suivante : https://www.cse-cst.gc.ca/fr/group-groupe/high-assurance-technologies.
Ancienne annexe F	Les exemples d'incidents COMSEC courants ont été retirés et se trouvent désormais à la section 16.8.
Ancienne annexe G	Le modèle de *Rapport initial d'incident COMSEC* a été retiré et se trouve désormais à l'adresse suivante : https://www.cse-cst.gc.ca/fr/group-groupe/high-assurance-technologies.
Section 1.10	La section *Demandes d'exception ou d'exemption* comprend une nouvelle exigence en matière d'examen annuel.
Section 1.12	Les numéros de téléphone sécurisé et de télécopieur sécurisé ont été ajoutés.
Sections 2.3 et 2.3.1	Ces sections ont été modifiées pour indiquer que le PSI assume dorénavant la responsabilité globale des services, qui était auparavant déléguée à la DSIC et à la DSII. Bien que les responsabilités précises de la DSIC soient détaillées dans le document, toutes les références à la DSII (section 2.3.2) ont été retirées.
Sections 5.1 et 5.5	Cette section a été mise à jour pour fournir au CCIC les critères d'ouverture et de fermeture d'un sous-compte COMSEC, y compris les exigences de base concernant l'habilitation de sécurité.
Section 5.1.1	Cette section a été reformulée pour indiquer que les Services à la clientèle en matière de COMSEC sont responsables de confirmer « l'inscription au PMC » et non « la conformité au PMC et à l'ITAR ».
Section 5.2.3	Cette section a été modifiée pour inclure les sous-systèmes manuels ainsi que les exigences relatives à la sauvegarde des systèmes.
Section 5.2.7	Le critère déterminant la « cote de fiabilité » permettant d'accéder au MCC a été retiré.

Référence	Modification
Section 5.3.2	Cette section a été modifiée de façon à supprimer l'exigence concernant l'envoi au Compte COMSEC industriel du CST et à éclaircir les modalités d'utilisation du formulaire *Demande de pouvoir de signature COMSEC*.
Section 6.2.5	Cette section a été modifiée de façon à clarifier la définition des CC 1 à 7.
Section 7.3.1	Cette section a été modifiée de façon à définir la différence entre la comptabilité locale du MCC dans le SNCMC et le suivi local du matériel COMSEC non comptable en dehors du SNCMC.
Section 7.9	Une responsabilité supplémentaire a été ajoutée aux avis de recherche.
Section 8.2.3	Cette section a été modifiée pour formuler une exigence visant la mise à jour des séances d'initiation COMSEC (tous les cinq ans) pour le personnel COMSEC actif.
Section 8.5	La modification indique que les représentants du CCIC (p. ex. les vérificateurs) n'ont PAS besoin de soumettre une demande de permis de visite, mais qu'en revanche, les membres du personnel du CCIC doivent coordonner les visites du CCIC avec le personnel du sous-compte COMSEC.
Section 9	Cette section a été modifiée pour fournir des clarifications et des critères obligatoires supplémentaires visant l'établissement et la protection des installations COMSEC.
Section 9.3.4	Une section concernant les « Incidents liés aux contenants de sécurité laissés sans surveillance » a été ajoutée.
Section 10.5	Une section concernant la « Distribution de clés électroniques sur support de stockage amovible magnétique ou optique » a été ajoutée.
Section 11.1.2	Deux nouveaux états de clé ont été ajoutés à cette section : l'état ROUGE (clés chiffrées) et l'état NOIR (clés non chiffrées).
Section 11.1.5	Une section concernant les copies de clés a été ajoutée.
Section 11.4.5	Une section contient un nouveau **nota** sur l'exigence de confirmer la réalisation des mises à niveau logicielles obligatoires.
Section 12.1	Cette section a été modifiée de façon à fournir des exigences de sécurité élémentaires au personnel effectuant la destruction du matériel COMSEC.
Section 13.2.1	L'inventaire « annuel » sera désormais l'inventaire « périodique ».
Section 14	Cette section concernant la planification COMSEC en cas d'urgence a été mise à jour.

NOTA : Il incombe à l'utilisateur de mettre en œuvre toutes les exigences de sécurité décrites dans la présente ITSD.

Table des matières

Avant-propos ..... **ii**

Résumé des modifications apportées à l'ITSD-06 aux fins de la présente ITSD ..... **iii**

Liste des tableaux ..... **viii**

Liste des figures ..... **viii**

1 Introduction **1**
1.1 Objet 1
1.2 Autorité 1
1.3 Portée 2
1.4 Contexte 2
1.5 Application 2
1.6 Résultats escomptés 2
1.7 Conformité 2
1.8 Conséquence de la non-conformité 3
1.9 Résolution de conflits 3
1.10 Demandes d'exception ou de dispense 3
1.11 Autres règlements liés à l'acquisition de matériel COMSEC 3
1.12 Coordonnées 4
1.13 Site Web du Centre de la sécurité des télécommunications 5

2 Rôles et responsabilités **5**
2.1 Généralités 5
2.2 Centre de la sécurité des télécommunications 5
2.3 Services publics et Approvisionnement Canada – Services de sécurité COMSEC dans le cadre de contrats 7
2.4 Centre de la sécurité des télécommunications – Services de sécurité COMSEC sans contrat géré par Services publics et Approvisionnement Canada 8
2.5 Ministère parrain du gouvernement du Canada – Entreprise du secteur privé 9
2.6 Entreprise du secteur privé 9

3 Sélection du personnel COMSEC **11**
3.1 Sélection du personnel de garde de sous-compte COMSEC 11
3.2 Titulaire de prêts 12

4 Formation **12**
4.1 Généralités 12
4.2 Formation sur l'équipement cryptographique 13
4.3 Formation des titulaires de prêts 13

5 Gestion des sous-comptes COMSEC **13**
5.1 Établissement d'un sous-compte COMSEC 13
5.2 Dossiers et documents 15
5.3 Changements à un sous-compte COMSEC 17
5.4 Absence du personnel de garde COMSEC 18
5.5 Fermeture d'un sous-compte COMSEC 19

5.6 Maintien d'un sous-compte COMSEC dont le solde est nul 20
5.7 Suspension d'un sous-compte COMSEC 20

6 Désignation du matériel COMSEC comptable 21
6.1 Généralités 21
6.2 Désignation 21
6.3 Inscription du matériel COMSEC dans le Système national de contrôle du matériel COMSEC 23
6.4 Types de matériel COMSEC comptable 24
6.5 Mentions spéciales et mises en garde 25
6.6 Matériel COMSEC non comptable 25

7 Registres, formulaires, rapports et avis comptables 26
7.1 Registre de contrôle du matériel COMSEC 26
7.2 Journal de contrôle du matériel COMSEC 26
7.3 Dossiers et registres comptables locaux 27
7.4 Rapports de matériel COMSEC 28
7.5 Rapport de conversion de clés de diversification 32
7.6 Rapport de remise à la clé opérationnelle 32
7.7 Rapport d'inventaire 32
7.8 Avis de recherche 32
7.9 Omission de répondre aux avis de recherche 33

8 Accès au matériel COMSEC comptable 33
8.1 Conditions préalables à l'accès au matériel COMSEC comptable 33
8.2 Séance d'initiation COMSEC et attestation d'initiation COMSEC 34
8.3 Intégrité par deux personnes 35
8.4 Zone jamais seul 35
8.5 Contrôle d'accès – Visites COMSEC 35
8.6 Demande de visite COMSEC 36

9 Sécurité physique 37
9.1 Installations COMSEC 37
9.2 Approbation de l'installation COMSEC 38
9.3 Entreposage sécurisé 39
9.4 Protection des combinaisons et des clés de serrures 40
9.5 Entreposage des clés cryptographiques 42
9.6 Entreposage de l'équipement cryptographique 44
9.7 Entreposage des publications COMSEC comptables 45

10 Distribution et réception du matériel COMSEC comptable 45
10.1 Généralités 45
10.2 Transfert à destination ou en provenance d'un intérêt étranger 45
10.3 Transmission de clés au moyen des systèmes de télécommunications 45
10.4 Distribution de matériel COMSEC comptable à l'extérieur d'un sous-compte 45
10.5 Distribution de clés électroniques sur support de stockage amovible magnétique ou optique 46
10.6 Suivi des envois de matériel COMSEC comptable 47
10.7 Emballage du matériel COMSEC comptable 48

10.8 Moyens de transport autorisés 50
10.9 Exigences relatives à la séparation 51
10.10 Messagers autorisés à transporter du matériel COMSEC comptable 51
10.11 Inspections douanières et préalables à l'embarquement 52
10.12 Transporteurs commerciaux 53
10.13 Réception du matériel COMSEC comptable 53

11 Manutention et utilisation du matériel COMSEC comptable 55
11.1 Clés cryptographiques 55
11.2 Équipement cryptographique 56
11.3 Publications COMSEC 60
11.4 Suivi local de matériel COMSEC non comptable 62

12 Disposition du matériel COMSEC comptable 63
12.1 Exigences générales 63
12.2 Autorisation 64
12.3 Destruction des clés 64
12.4 Destruction de l'équipement cryptographique, des publications, des supports de stockage amovibles et des clés matérielles comptables 64
12.5 Réalisation de la destruction courante des clés 65
12.6 Méthodes de destruction courante 66

13 Inventaire de sous-compte COMSEC 67
13.1 Motifs de l'inventaire 67
13.2 Types d'inventaire 67
13.3 Rapports d'inventaire 68
13.4 Processus d'inventaire 69

14 Planification COMSEC en cas d'urgence 70
14.1 Exigence 70
14.2 Planification en cas de catastrophes naturelles et d'urgences 71
14.3 Plan d'urgence 71
14.4 Planification des mesures d'urgence 72

15 Vérification des sous-comptes COMSEC 72
15.1 Planification de la vérification 72
15.2 Réalisation de la vérification 73
15.3 Rapports de vérification 74

16 Incidents COMSEC 74
16.1 Généralités 74
16.2 Traitement des incidents 75
16.3 Rapport initial d'incident COMSEC 75
16.4 Rapport d'évaluation d'incident COMSEC 75
16.5 Rapport détaillé 76
16.6 Rapport d'évaluation finale et de clôture 76
16.7 Classification et diffusion des rapports 76
16.8 Exemples d'incidents COMSEC 77

17 Références 79

17.1 Liste d'acronymes, d'abréviations et de sigles....79
17.2 Glossaire....81

18 Bibliographie....A-87

Annexe A Rôles et responsabilités liés au sous-compte COMSEC....A-1
A.1 Gardien de sous-compte COMSEC....A-1
A.2 Gardien suppléant de sous-compte COMSEC....A-2
A.3 Titulaire de prêts....A-2

Annexe B Procédures de réception du matériel COMSEC comptable....B-1
B.1 Préparation en prévision de la réception du matériel COMSEC comptable....B-1
B.2 Inspection des colis....B-1
B.3 Équipement cryptographique scellé....B-1

Annexe C Acquisition d'équipement cryptographique comptable....C-1
C.1 Généralités....C-1
C.2 Acquisition en vertu d'un contrat du gouvernement du Canada....C-1
C.3 Acquisition sans contrat du gouvernement du Canada....C-1
C.4 Installation de l'équipement cryptographique comptable....C-2
C.5 Exigences relatives aux clés....C-2
C.6 Procédure d'acquisition....C-2

Annexe D Rôles et responsabilités – Guide de référence....D-1
D.1 Rôles et responsabilités – Avec un contrat du gouvernement du Canada....D-1
D.2 Rôles et responsabilités – Sans contrat du gouvernement du Canada....D-6

Liste des tableaux

Tableau 1 – Coordonnées des bureaux COMSEC....4

Tableau 2 – Dossiers administratifs et exigences de conservation....16

Tableau 3 – Rédaction du *Journal de contrôle du matériel COMSEC*....27

Tableau 4 – Entreposage des clés physiques....42

Tableau 5 – Clés gardées en réserve....44

Tableau 6 – Moyens de transport autorisés pour le matériel COMSEC comptable....54

Tableau 7 – Rôles et responsabilités – Avec un contrat du gouvernement du Canada....D-1

Liste des figures

Figure 1 – Système national de contrôle du matériel COMSEC (pour ce qui a trait aux entreprises du secteur privé)....7

1 Introduction

Le gouvernement du Canada (GC) a établi un programme sur la sécurité des communications (COMSEC pour *Communications Security*) qui a pour objet de favoriser la protection de l'information classifiée et PROTÉGÉ C. Ce programme COMSEC porte sur l'application de mesures de sécurité cryptographique, de sécurité des transmissions et des émissions ainsi que de sécurité physique, de même que sur les pratiques opérationnelles et les mécanismes de contrôle connexes. La COMSEC vise à empêcher tout accès non autorisé à l'information et aux données issues de télécommunications ainsi qu'à garantir l'authenticité de ces télécommunications.

Aux fins de la présente directive, le terme « ministère du GC » comprend toutes les institutions fédérales (p. ex. ministères, agences et organismes) assujetties à la *Politique sur la sécurité du gouvernement* (PSG) et figurant aux annexes I, I.1, II, IV et V de la *Loi sur la gestion des finances publiques* (LGFP), à l'exception de celles qui sont expressément exclues en vertu d'une loi, d'un règlement ou d'un décret.

Le « matériel COMSEC » sert à sécuriser ou à authentifier l'information de télécommunication. Il inclut les clés cryptographiques, les dispositifs, le matériel informatique et les micrologiciels ou logiciels qui mettent en application ou décrivent une logique cryptographique. Il comprend également les documents qui décrivent ces éléments ou qui en orientent les mesures de soutien.

L'application de cette directive permet d'assurer le respect des contrôles de sécurité du GC lorsqu'une entreprise du secteur privé canadien se voit octroyer l'accès à du matériel COMSEC du gouvernement.

1.1 Objet

La présente directive énonce les exigences minimales en matière de sécurité que doivent respecter les praticiens COMSEC dans le cadre du contrôle et de la gestion du matériel COMSEC autorisé par le Centre de la sécurité des télécommunications (CST) aux fins d'utilisation, au Canada, par une entreprise du secteur privé canadien (désignée ci-après sous l'appellation « entreprise du secteur privé »).

Aux fins de la présente directive, le terme « praticien COMSEC » englobe les autorités COMSEC des ministères et du secteur privé (parrains et planificateurs), ainsi que le personnel de garde chargé de gérer et de contrôler le matériel COMSEC comptable au sein d'un compte COMSEC.

NOTA 1 : Afin d'obtenir des directives concernant l'établissement d'un sous-compte COMSEC pour une entreprise du secteur privé située à l'extérieur du Canada, prière de communiquer avec les Services à la clientèle en matière de COMSEC.

NOTA 2 : Aux fins de la présente directive, le terme « entreprise du secteur privé » englobe les organisations, les entreprises ou les personnes canadiennes qui ne sont pas visées par la LGFP et qui ne relèvent pas d'un gouvernement provincial ou municipal.

1.2 Autorité

La présente directive est promulguée au titre de la PSG, en vertu de laquelle le CST constitue l'autorité nationale en matière de COMSEC. Le CST est responsable de l'élaboration, de l'approbation et de la promulgation des instruments de politique visant la COMSEC, ainsi que de la conception des lignes directrices et des outils s'appliquant à la sécurité des technologies de l'information (TI).

Au CST, le chef adjoint de la Sécurité des TI est responsable de la promulgation des instruments de politique relatifs à la COMSEC.

1.3 Portée

Les méthodes de contrôle varient selon la nature du matériel COMSEC.

La portée de la présente directive concerne les deux types de matériel suivants :

- le matériel COMSEC contrôlé et comptabilisé conformément au Système national de contrôle du matériel COMSEC (SNCMC) ainsi que le matériel COMSEC faisant l'objet d'un suivi local assuré par le gardien de sous-compte COMSEC au moyen d'un registre manuel ou électronique qui n'est toutefois pas assujetti au SNCMC, mais qui est approuvé par le CST;
- le matériel COMSEC nécessitant une manutention spéciale qui est définie dans l'*International Traffic in Arms Regulations* (ITAR) des États-Unis ainsi que dans le *Règlement sur les marchandises contrôlées* (RMC) régi par le Programme des marchandises contrôlées (PMC) du Canada.

1.4 Contexte

La présente directive favorise l'application de la PSG et de la *Directive sur la gestion de la sécurité ministérielle* (DGSM), et devrait être lue parallèlement aux publications suivantes :

- *Directive en matière de sécurité des TI sur l'application de la sécurité des communications à l'aide de solutions approuvées par le CST* (ITSD-01A), janvier 2014;
- *Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* (ITSD-03A), mars 2014;
- *Directive en matière de sécurité des TI sur le contrôle et la gestion du matériel COMSEC en cours de réalisation* (ITSD-08), en cours d'élaboration en 2016;
- *Directive sur le signalement et l'évaluation des incidents COMSEC touchant le matériel COMSEC comptable* (ITSD-05), avril 2012;
- *Manuel de la sécurité industrielle* (MSI).

1.5 Application

La présente directive s'applique aux entreprises du secteur privé autorisées à manutentionner, à contrôler et à protéger le matériel COMSEC approuvé par le CST suivant une entente de parrainage (c.-à-d. un contrat conclu avec le GC par l'intermédiaire de Services publics et Approvisionnement Canada [SPAC] ou encore tout autre type d'accord approuvé par le CST).

1.6 Résultats escomptés

L'application de la présente directive permettra de protéger l'information ainsi que les données classifiées et protégées du GC. Elle permettra également d'harmoniser les engagements du Canada en matière de contrôle et de protection du matériel COMSEC avec les ententes et les exigences de sécurité de ses partenaires internationaux.

1.7 Conformité

Il incombe au Compte COMSEC industriel du CST (CCIC), au ministère parrain du GC et à l'entreprise concernée du secteur privé de se conformer aux exigences de sécurité minimales énoncées dans la présente directive.

Avant d'être autorisée à ouvrir un sous-compte COMSEC, une entreprise du secteur privé parrainée doit s'engager, en vertu d'une *Entente de contrôle du matériel COMSEC comptable* (ECMCC), à mettre en œuvre les exigences et les contrôles de gestion prescrits par la présente directive, ainsi que les contrôles et les exigences de gestion connexes que le CST juge nécessaires.

1.8 Conséquence de la non-conformité

La non-conformité à la présente directive peut donner lieu à une escalade des contrôles administratifs exercés sur le sous-compte COMSEC de ladite entreprise du secteur privé. En dernier recours, après maintes occurrences de non-conformité, le sous-compte COMSEC sera suspendu ou fermé jusqu'à ce que le CCIC effectue une vérification externe et que les lacunes en matière de COMSEC soient corrigées.

1.9 Résolution de conflits

La présente directive vise à donner un sommaire détaillé des obligations relatives au contrôle et à la manutention du matériel COMSEC approuvé par le CST au sein des entreprises du secteur privé. Elle doit être lue en parallèle avec le *Manuel de la sécurité industrielle* (MSI) de Services publics et Approvisionnement Canada.

Toute divergence entre un énoncé d'exigence contenu dans la présente ITSD et une exigence à l'échelle nationale (p. ex. PSG, DGSM, MSI et *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* [GSTI]) ou internationale (p. ex. ITAR) doit être signalée aux Services à la clientèle en matière de COMSEC aux fins de résolution.

Advenant un conflit avec une autre directive COMSEC (p. ex. une directive en matière de sécurité des technologies de l'information [ITSD pour *Information Technology Security Directive*]), la présente directive a préséance.

1.10 Demandes d'exception ou de dispense

L'agent de sécurité de l'entreprise (ASE) doit soumettre les demandes d'exception (substitution) ou de dispense (exemption temporaire à une exigence donnée) au CCIC, qui les acheminera à son tour aux Services à la clientèle en matière de COMSEC du CST. Les demandes doivent être présentées par écrit et comprendre une justification. Les Services à la clientèle en matière de COMSEC assureront la coordination de toutes les demandes d'exception et de dispense auprès des organismes parrains, selon le cas.

NOTA : Les exceptions et les dispenses sont revues périodiquement par les Services à la clientèle en matière de COMSEC.

1.11 Autres règlements liés à l'acquisition de matériel COMSEC

1.11.1 Propriété, contrôle et influence de l'étranger

Une entreprise du secteur privé doit normalement faire l'objet d'une évaluation liée à la propriété, au contrôle et à l'influence de l'étranger (PCIE) réalisée par le Programme de sécurité industrielle (PSI) de SPAC avant de pouvoir accéder à du matériel COMSEC comptable (MCC) en vue de s'acquitter de ses responsabilités contractuelles en matière de produits livrables ou de satisfaire à une exigence approuvée par le CST. Cette évaluation vise à s'assurer qu'il n'existe, ni dans les titres de propriété ni dans les mécanismes de contrôle de l'entreprise, d'éléments pouvant constituer un risque, advenant l'octroi d'accès à du MCC.

Ainsi, on considérera qu'une entreprise du secteur privé fait l'objet d'une évaluation PCIE défavorable de SPAC lorsqu'il y a un motif raisonnable de croire que la nature et la portée de la propriété, du contrôle et de l'influence étrangers exercent, sur les activités de gestion et d'exploitation de l'installation, une pression pouvant permettre à des tiers étrangers ou à leurs représentants d'accéder illicitement à du MCC.

NOTA : Les demandes d'exemption d'une évaluation PCIE doivent être présentées aux Services à la clientèle en matière de COMSEC.

1.11.2 Programme des marchandises contrôlées du Canada

Le Programme des marchandises contrôlées (PMC) canadien est un programme national de sécurité industrielle de SPAC qui, en vertu du RMC, a le mandat de renforcer les mesures de contrôle relatives au commerce de défense du Canada et d'empêcher la prolifération de biens tactiques et stratégiques.

L'acceptation des exigences de contrôle et de gestion du MCC détaillées dans la présente directive et dans d'autres directives du CST (y compris les ECMCC, les protocoles d'entente [PE], les protocoles d'accord [PA], les ententes de non-divulgation et les accords d'assistance technique [AAT]) n'exempte pas une entreprise du secteur privé de l'obligation de mettre en œuvre les exigences du PMC canadien.

1.11.3 International Traffic in Arms Regulations des États-Unis

L'ITAR est un ensemble de règlements du gouvernement américain qui régissent l'exportation et l'importation des biens et services de défense énumérés dans la *United States Munitions List* (USML).

Une quantité importante de matériel COMSEC du GC provient des États-Unis. L'acceptation des exigences de contrôle et de gestion du MCC énoncées dans la présente directive et dans les autres directives du CST (y compris les ECMCC, les PE, les PA et les ententes de non-divulgation) n'exempte pas une entreprise du secteur privé de l'obligation de mettre en œuvre les exigences de l'ITAR. Pour des conseils et des directives concernant le déplacement de MCC assujetti au contrôle ITAR, prière de communiquer avec les Services à la clientèle en matière de COMSEC.

1.12 Coordonnées

Le tableau ci-dessous contient les coordonnées des bureaux offrant un soutien COMSEC aux utilisateurs.

NOTA : Sauf indication contraire, les bureaux du CST reçoivent les appels téléphoniques et les transmissions par télécopieur du lundi au vendredi, de 8 h à 16 h (heure de l'Est).

Tableau 1 – Coordonnées des bureaux COMSEC

Bureau	Numéro de téléphone	Adresse électronique
Compte COMSEC industriel du CST (CCIC)	Téléphone : 613-991-7272 Téléphone sécurisé : 613-991-7597 Télécopieur sécurisé : 613-991-7593	cica-ccic@cse-cst.gc.ca
Services à la clientèle en matière de COMSEC	Téléphone : 613-991-8495	comsecclientservices@cse-cst.gc.ca

1.13 Site Web du Centre de la sécurité des télécommunications

Des directives COMSEC additionnelles, des formulaires ainsi que de l'information (au niveau NON CLASSIFIÉ seulement) ayant trait aux produits, systèmes et services d'assurance élevée approuvés par le CST sont disponibles à l'adresse suivante : https://www.cse-cst.gc.ca/fr/group-groupe/high-assurance-technologies.

2 Rôles et responsabilités

2.1 Généralités

La présente section traite des principaux rôles et responsabilités du CST, des ministères parrains du GC et des entreprises du secteur privé pour ce qui concerne la gestion du matériel COMSEC au sein des entreprises du secteur privé. Elle décrit également les fonctions de sécurité du PSI de SPAC dans le contexte d'un contrat du GC.

NOTA : L'annexe D contient un guide de référence sur les rôles et responsabilités énoncés dans la présente directive.

2.2 Centre de la sécurité des télécommunications

Le CST est l'autorité nationale COMSEC. À ce titre, il est responsable d'approuver la certification, l'acquisition et l'utilisation de l'équipement et des clés cryptographiques, ainsi que les instruments de politique liés à la COMSEC qui protègent l'information et les données classifiées et PROTÉGÉ C.

2.2.1 Services à la clientèle en matière de COMSEC

Sous la direction du chef adjoint, Sécurité des technologies de l'information (CA STI), les Services à la clientèle en matière de COMSEC sont responsables de fournir au GC et aux entreprises du secteur privé des conseils, de l'orientation et des directives visant les solutions et la manutention du matériel COMSEC approuvées par le CST. En ce qui a trait aux entreprises du secteur privé, les responsabilités des Services à la clientèle en matière de COMSEC incluent ce qui suit :

- évaluer la pertinence de la présentation en bonne et due forme d'une soumission en vue d'obtenir un contrat (p. ex. une *demande de propositions* [DP]) par une entreprise qui n'est pas déjà titulaire d'un sous-compte COMSEC (voir la section 8.1.3);
- autoriser l'établissement ou la fermeture d'un sous-compte COMSEC;
- établir si une entreprise du secteur privé est en mesure de justifier son recours à des solutions et à du matériel COMSEC approuvés par le CST;
- confirmer, notamment au moyen d'inspections et de vérifications, qu'une entreprise du secteur privé satisfait à tous les préalables de sécurité avant d'autoriser la remise de MCC au sous-compte COMSEC qui la représente; les vérifications suivantes sont donc prévues :
  - attestation de sécurité d'installation (ASI) ou l'équivalent;
  - inspection liée à l'autorisation de détenir des renseignements (ADR) ou l'équivalent;
  - inspection des mesures de protection COMSEC (IMPC);
  - inspection de la production (pour les exigences liées au matériel COMSEC en cours de réalisation [IP pour *In-Process*] – voir l'ITSD-08);
  - évaluation PCIE (voir la section 1.11.1) ou exemption;

- coordonner la signature des ECMCC, des AAT, des ententes de non-divulgation et d'autres accords, le cas échéant;
- valider les plans de soutien liés au matériel de chiffrement (PSMC) (voir la *Directive sur l'utilisation de l'équipement COMSEC et des clés approuvés par le CSTC dans un réseau de télécommunication* [ITSD-04]), le cas échéant;
- coordonner la réalisation des inspections TEMPEST;
- coordonner les expéditions transfrontalières de MCC avec les autres autorités responsables de la sécurité nationale.

2.2.2 Autorité COMSEC du ministère du Compte COMSEC industriel du CST

Relevant du CA STI, l'autorité COMSEC du ministère (ACM) du CCIC est chargée d'élaborer, de mettre en œuvre, de maintenir, de coordonner et de surveiller un programme COMSEC du secteur privé qui soit conforme à la PSG et aux instruments de politique connexes ayant trait à la gestion COMSEC. De plus, l'ACM du CCIC est responsable du contrôle global du matériel COMSEC approuvé par le CST dont le CCIC a la charge.

2.2.3 Compte COMSEC industriel du CST

Dirigé par l'ACM du CCIC, le CCIC est responsable de la gestion et du contrôle des solutions et du matériel COMSEC que le CST a approuvés et attribués aux sous-comptes COMSEC du secteur privé. Au nombre des responsabilités du CCIC, notons les suivantes :

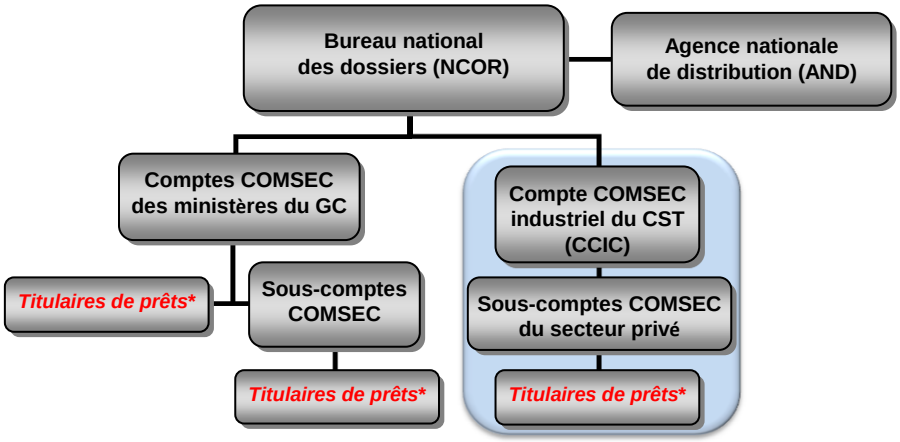
- remplir la fonction de personne-ressource initiale en ce qui a trait à la gestion des comptes COMSEC IP et des sous-comptes COMSEC (y compris le signalement des incidents COMSEC);
- ouvrir et fermer les sous-comptes COMSEC des entreprises du secteur privé conditionnellement à l'approbation des Services à la clientèle en matière de COMSEC;
- veiller au respect des règles de gestion du MCC en plus de soutenir et d'orienter l'utilisation des clés et de l'équipement cryptographiques approuvés par le CST;

  NOTA : Dans le reste du document (à l'exception du glossaire), le terme « clé » sera employé pour désigner le terme « clé cryptographique ». Il inclut toutes les formes de clés physiques ou électroniques.
- effectuer le rapprochement annuel de l'inventaire des sous-comptes COMSEC;
- effectuer les vérifications des sous-comptes COMSEC des entreprises du secteur privé (voir la section 15);
- autoriser et coordonner le déplacement ainsi que la distribution du MCC à l'échelle du pays (fournir des ordres de mission de messager, le cas échéant).

2.2.4 Système national de contrôle du matériel COMSEC

Le SNCMC est le système logistique national de MCC approuvé par le CST qui comprend le personnel et les procédures permettant aux ministères du GC et aux entreprises du secteur privé de manutentionner et de contrôler efficacement le MCC. Le SNCMC assure le contrôle du MCC par l'intermédiaire des éléments suivants :

- le Bureau national des dossiers (NCOR pour *National Central Office of Record*);
- l'Agence nationale de distribution (AND);
- les comptes COMSEC;
- les sous-comptes COMSEC;
- les titulaires de prêts.



*Nouvelle terminologie : anciennement appelés « éléments locaux » ou « détenteurs d'accusé de réception ».

Figure 1 – Système national de contrôle du matériel COMSEC (pour ce qui a trait aux entreprises du secteur privé)

2.2.5 Bureau national des dossiers

Le NCOR est l'entité du CST qui est chargée de superviser la gestion et la comptabilité du MCC produit ou confié au Canada. Le NCOR assume trois rôles distincts : autorité d'inscription, gestionnaire de compte COMSEC et gestionnaire des certificats de privilèges du processeur de clés (KP pour *Key Processor*). Ces rôles sont administrés par le Centre d'assistance en matière de matériel cryptographique (CAMC).

2.2.6 Agence nationale de distribution

L'AND est l'entité du CST qui est responsable de la réception et de la distribution du MCC en provenance et à destination du Canada.

2.3 Services publics et Approvisionnement Canada – Services de sécurité COMSEC dans le cadre de contrats

Le Secteur de la sécurité industrielle (SSI) de SPAC veille à l'application des mesures de sécurité à toutes les étapes de la passation des contrats avec les entreprises du secteur privé, conformément à ce qui est stipulé dans le PSI et la PSG. Le PSI permet aux entreprises du secteur privé canadien de soumissionner pour les contrats nationaux et internationaux du gouvernement, et assure la sécurité du public en protégeant les biens sensibles et contrôlés. Il offre également des services de sécurité dans le cadre de contrats.

2.3.1 Programme de sécurité industrielle

Aux entreprises du secteur privé canadien qui ont obtenu un contrat ou un sous-contrat avec SPAC (national ou international) et qui doivent accéder à de l'information ou à des biens protégés ou classifiés du gouvernement, le PSI offre les services suivants :

- services d'enquête de sécurité sur le personnel;
- inspections liées à la sécurité des TI, à la production, à la sécurité physique et à l'ADR sur le site;
- conditions d'utilisation visant la sécurité et devant figurer dans les contrats;

- réalisation des ASI;
- évaluations PCIE (voir la section 1.11.1);
- vérification de sécurité des entreprises et du personnel du secteur privé conformément aux exigences de sécurité des contrats étrangers de l'Organisation du Traité de l'Atlantique Nord (OTAN);
- transfert, par voie intergouvernementale, d'information et de biens non COMSEC protégés et classifiés entre les gouvernements canadien et étrangers, et le secteur privé;
- élaboration d'instructions de sécurité des projets (ISP) d'envergure internationale, dont celles qui concernent les exigences COMSEC;
- demandes de visites, pour veiller au respect des exigences relatives aux visites de sécurité (voir les exigences en matière d'accès au matériel COMSEC à la section 8.6) dans le cadre des visites d'organismes gouvernementaux ou d'entreprises du secteur privé au Canada ou à l'étranger.

2.4 Centre de la sécurité des télécommunications – Services de sécurité COMSEC sans contrat géré par Services publics et Approvisionnement Canada

Lorsqu'il n'y a pas de contrat géré par SPAC et qu'une entreprise du secteur privé doit accéder à du MCC (provenant habituellement d'un pays étranger), les services de sécurité sont les mêmes que ceux détaillés dans la présente directive, à l'exception des exigences en matière de parrainage et de PCIE (voir le NOTA ci-dessous).

Les Services à la clientèle en matière de COMSEC s'assureront que l'entreprise du secteur privé canadien a établi un sous-compte COMSEC relevant du CCIC, qui soit doté de capacités équivalentes à l'ASI, à l'ADR et à l'IMPC.

Il incombe aux partenaires de l'industrie étrangère de demander aux responsables de leur propre secrétariat d'État (DoS pour *Department of State*) que du MCC soit distribué à une entreprise du secteur privé canadien. Une fois qu'ils ont obtenu la preuve que les responsables du secrétariat d'État étranger ont bien reçu la demande, les Services à la clientèle en matière de COMSEC coordonnent la distribution du MCC avec les responsables du secrétariat d'État et les responsables COMSEC étrangers. Cette distribution est conditionnelle à l'obtention d'une approbation écrite officielle autorisant la distribution du MCC à l'entreprise du secteur privé canadien.

Le déplacement interfrontalier (exportation ou importation) de tout MCC doit être effectué par l'entremise de l'AND canadienne du CST, et le matériel est manutentionné au Canada par les voies COMSEC nationales (p. ex. SNCMC). Avant la distribution du matériel, les Services à la clientèle en matière de COMSEC s'assurent que l'entreprise du secteur privé canadien a établi un sous-compte COMSEC relevant du CCIC, qui répond aux exigences liées à l'ASI, à l'ADR et à l'IMPC.

NOTA : La déclaration de distribution écrite officielle des responsables du DoS et des responsables COMSEC étrangers indiquera que ceux-ci acceptent la distribution sans la conduite d'une évaluation PCIE canadienne. Après l'établissement de la distribution, les Services à la clientèle en matière de COMSEC exempteront l'entreprise du secteur privé de l'exigence relative au ministère parrain du GC, tel qu'il est décrit à la section 2.5.

2.5 Ministère parrain du gouvernement du Canada – Entreprise du secteur privé

Une entreprise du secteur privé doit être parrainée par un ministère du GC (désigné ci-après sous l'appellation « parrain du GC ») qui possède un compte COMSEC en règle avant d'avoir accès à du MCC. L'ACM du parrain du GC est responsable de ce qui suit :

- informer les Services à la clientèle en matière de COMSEC qu'une entreprise du secteur privé a besoin d'accéder à du MCC;

  NOTA : Cette mesure doit être prise le plus tôt possible dans le processus d'attribution du contrat et de définition des besoins, afin d'établir les exigences de gestion du matériel COMSEC, de façon à respecter les délais.

- signer l'ECMCC à titre de ministère parrain;
- confirmer qu'une entreprise du secteur privé est inscrite auprès du PMC avant de lui confier le MCC;
- s'assurer que les Services à la clientèle en matière de COMSEC ont reçu la liste approuvée de vérification des exigences relatives à la sécurité (LVERS) du contrat, y compris les modifications, le cas échéant;
- fournir des inspections équivalentes aux inspections liées à l'ASI, à l'ADR et aux TI, ainsi que des évaluations PCIE (comme l'exige le CST) pour les entreprises parrainées qui ne sont pas assujetties à un contrat du GC;
- fournir les documents pertinents additionnels (tel que l'exige le CST) pour les entreprises parrainées qui ne sont pas assujetties à un contrat du GC;
- déterminer les besoins en matière de MCC et présenter aux Services à la clientèle en matière de COMSEC une *Demande d'équipement COMSEC* (DEC) et une *Demande d'autorisation pour l'achat d'équipement COMSEC* (DAAEC) dûment remplies, le cas échéant;
- assigner une autorité de contrôle (ConAuth) pour les réseaux cryptographiques autorisés, le cas échéant (voir l'ITSD-04);
- coordonner, avec le CCIC, la distribution du MCC à l'entreprise du secteur privé une fois que toutes les conditions préalables à l'établissement d'un sous-compte COMSEC ont été remplies (voir la section 5.1);
- coordonner, avec le CCIC, le retrait de fin de contrat de tout le MCC de l'entreprise du secteur privé.

2.6 Entreprise du secteur privé

2.6.1 Président-directeur général ou cadre supérieur désigné

Le président-directeur général (PDG) ou cadre supérieur désigné (également désigné ci-après sous l'appellation « PDG ») d'une entreprise du secteur privé est chargé de nommer un ASE. Il convient de suivre les procédures énoncées dans le MSI lorsque l'entreprise du secteur privé souhaite s'inscrire au PSI.

2.6.2 Agent de sécurité de l'entreprise

L'ASE rend compte au PDG de la posture globale de la sécurité COMSEC de l'entreprise. Les responsabilités relatives au contrôle et à la gestion COMSEC de l'ASE pour le MCC incluent ce qui suit :

- coordonner la signature des ECMCC par un cadre supérieur de l'entreprise;
- veiller à la gestion des biens de MCC conformément aux prescriptions de la présente directive et tel qu'il est exigé par le CCIC;

- veiller au respect des exigences de l'ITAR (voir la section 1.11.3), de la PCIE (voir la section 1.11.1) et du PMC canadien (voir la section 1.11.2);
- nommer le gardien de sous-compte COMSEC et le gardien suppléant de sous-compte COMSEC (désigné ci-après sous l'appellation « gardien suppléant ») de l'entreprise;
- veiller à ce qu'un membre du personnel COMSEC (gardien de sous-compte ou gardien suppléant) soit disponible en permanence pour répondre aux besoins du sous-compte;
- veiller à ce que le personnel de garde du sous-compte COMSEC reçoive une formation officielle du CST en gestion du matériel COMSEC;
- confirmer que les exigences relatives à la gestion COMSEC sont intégrées aux consignes de sécurité de l'entreprise;
- confirmer qu'il existe une ASI – ou un équivalent de niveau approprié – et que des inspections liées aux TI, à l'ADR et à la production – ou un équivalent – ont été effectuées avant d'accepter le MCC;
- veiller à ce que des séances d'initiation COMSEC soient offertes au personnel qui doit accéder au MCC;
- traiter les demandes de visite COMSEC (c.-à-d. les visites nécessitant un accès au MCC) dans le cadre d'un contrat, tel qu'il est énoncé dans le MSI et dans la présente directive; les demandes d'habilitation de sécurité des visiteurs doivent être présentées par l'entremise du PSI; le personnel du PSI demande ensuite une autorisation d'accès COMSEC aux Services à la clientèle en matière de COMSEC;
- s'assurer de recevoir l'autorisation de visite du PSI avant de permettre aux visiteurs d'accéder au MCC;
- élaborer un *plan d'urgence COMSEC* (voir la section 14);
- signaler les incidents COMSEC au CCIC (voir la section 16 et l'ITSD-05);
- veiller à ce que les sous-traitants respectent les exigences de sécurité du PSI ou de son équivalent et de la présente directive avant de leur permettre d'accéder au MCC.

2.6.3 Séparation des tâches

Le PDG ou l'ASE ne doit pas occuper le poste de gardien de sous-compte COMSEC ou de gardien suppléant pour l'entreprise.

Sauf dans le cas d'un compte COMSEC IP, le gardien de sous-compte COMSEC ou son gardien suppléant ne peuvent gérer plus d'un sous-compte COMSEC à la fois.

2.6.4 Gardien de sous-compte COMSEC

Le gardien de sous-compte COMSEC est responsable de la réception, de la garde, de la distribution, de la disposition, de la destruction et de la comptabilité du MCC porté à son sous-compte COMSEC, conformément à la présente directive et tel qu'il est exigé par le CCIC. Prière de consulter l'Annexe A pour la liste détaillée des tâches du gardien de sous-compte COMSEC.

2.6.5 Gardien suppléant de sous-compte COMSEC

Le gardien suppléant a pour rôle d'assister le gardien de sous-compte COMSEC dans ses tâches quotidiennes en lien avec un sous-compte COMSEC et d'exercer les fonctions du gardien en l'absence temporaire de ce dernier. Prière de consulter l'Annexe A pour la liste détaillée des tâches du gardien suppléant.

2.6.6 Titulaire de prêts

Un titulaire de prêts est une personne autorisée à détenir, à conserver et à utiliser du MCC. Il est également autorisé à échanger du MCC uniquement avec le sous-compte COMSEC auquel il est inscrit. Un titulaire de prêts ne peut pas être inscrit à plus d'un sous-compte à la fois et n'est pas autorisé à prêter du MCC. Voir la liste détaillée des tâches d'un titulaire de prêts à l'Annexe A.

2.6.7 Travailleurs de quart et personnel technique

Dans certains cas, il est possible que des personnes comme un travailleur de quarts ou un technicien (désigné ci-après sous l'appellation « utilisateur autorisé ») nécessitent un accès à court terme (immédiat) au MCC (ce qui n'est pas considéré comme un prêt). Avant d'accorder cet accès, le gardien de sous-compte doit s'assurer que l'utilisateur autorisé répond aux exigences stipulées à la section 8.1 de même qu'à celles qui sont énoncées ci-dessous :

- être un employé de l'entreprise;
- avoir lu et signé le formulaire *Responsabilités du titulaire de prêts*;
- avoir signé un accusé de réception pour le MCC et conserver celui-ci sous son contrôle personnel constant jusqu'à ce qu'il doive le retourner;
- retourner le MCC qui n'est pas utilisé pour qu'il soit mis sous clé;
- s'abstenir de transporter le MCC dans une autre aire de travail ou dans un autre immeuble à moins d'avoir obtenu le consentement du gardien de sous-compte COMSEC ou du titulaire de prêts;
- comprendre ce qui constitue un incident COMSEC ou un incident COMSEC potentiel (voir l'ITSD-05).

2.6.8 Personnel témoin

Un employé de l'entreprise – autre qu'un membre du personnel de garde – peut être nommé comme témoin des transactions effectuées au compte (p. ex. les *rapports de possession, d'inventaire* et *de destruction*). Le témoin doit avoir satisfait aux conditions préalables d'accès au MCC et posséder une habilitation de sécurité de niveau égal ou supérieur au niveau de classification le plus élevé de la transaction de MCC dont il est le témoin.

NOTA : Une personne ne peut en aucun cas être autorisée à signer comme témoin d'une transaction sans avoir vu le MCC en question.

3 Sélection du personnel COMSEC

3.1 Sélection du personnel de garde de sous-compte COMSEC

L'ASE doit effectuer un contrôle rigoureux des personnes appelées à remplir le rôle de gardien de sous-compte COMSEC ou de gardien suppléant. En l'occurrence, il doit s'assurer que les candidats répondent aux critères suivants :

- être un citoyen canadien (qui peut avoir une double nationalité);
- être un employé de l'entreprise;
- posséder une habilitation de sécurité égale ou supérieure au niveau de sensibilité le plus élevé du MCC détenu au sous-compte COMSEC, mais jamais inférieure au niveau SECRET;

- posséder une attestation d'initiation COMSEC à jour (voir la section 8.2);
- être une personne responsable apte à assumer les fonctions et les responsabilités de gardien de sous-compte COMSEC ou de gardien suppléant;
- occuper un poste ou posséder le niveau décisionnel qui lui donne les pouvoirs nécessaires pour exercer les responsabilités du poste;
- n'avoir jamais été relevé de ses fonctions en tant que gardien de sous-compte COMSEC ou de gardien suppléant pour cause de négligence ou de manquement au devoir;
- ne pas exercer de charges additionnelles qui puissent nuire à ses fonctions de gardien de sous-compte COMSEC ou de gardien suppléant de l'entreprise.

3.2 Titulaire de prêts

Le gardien de sous-compte COMSEC doit s'assurer que des titulaires de prêts sont nommés à des fins opérationnelles, pour peu que ces fins nécessitent le recours ou l'accès à du MCC. En plus de satisfaire aux critères énoncés à la section 2.6.6 et à l'Annexe A.3, le titulaire de prêts doit répondre aux exigences suivantes :

- être un citoyen canadien (qui peut avoir une double nationalité);
- être un employé de l'entreprise pour laquelle le sous-compte COMSEC a été établi, à moins que les Services à la clientèle en matière de COMSEC n'autorisent formellement d'autres dispositions;
- n'avoir jamais été relevé de ses fonctions en tant que titulaire de prêts pour négligence ou manquement au devoir;
- posséder une habilitation de sécurité égale ou supérieure au niveau de sensibilité le plus élevé du MCC détenu;
- occuper un poste ou posséder le niveau décisionnel qui donne les pouvoirs nécessaires pour exercer les responsabilités du poste.

4 Formation

4.1 Généralités

Avant d'occuper leurs postes respectifs, c'est-à-dire avant d'administrer les tâches du sous-compte COMSEC, les gardiens de sous-compte COMSEC et les gardiens suppléants doivent suivre la formation de gardien COMSEC du CST. Les anciens gardiens de sous-compte COMSEC ou gardiens suppléants qui n'ont pas exercé de fonctions liées à la COMSEC depuis plus de deux ans doivent également suivre une formation COMSEC officielle.

NOTA : Le gardien de sous-compte COMSEC ou le gardien suppléant doit s'assurer que les titulaires de prêts et les utilisateurs autorisés de MCC reçoivent tous une formation qui leur permettra de contrôler et de gérer adéquatement le MCC qu'ils auront en leur possession.

4.1.1 Formation COMSEC du CST

Le calendrier de formation et les modalités d'inscription au cours de gardien COMSEC du CST sont disponibles auprès du Centre de formation en sécurité des TI (CFSTI). Le CCIC doit recevoir une attestation confirmant que le cours a été suivi.

NOTA : Le personnel qui doit accéder au MCC et qui suit la formation doit obtenir au préalable une attestation d'initiation COMSEC.

4.1.2 Formation sur les systèmes de comptabilité COMSEC

Avant d'installer et d'utiliser un système ou un progiciel de comptabilité automatisé qui a été approuvé par le CST aux fins de gestion du MCC, le gardien de sous-compte COMSEC et le gardien suppléant doivent suivre une formation officielle du CST sur ledit système ou progiciel, si elle est offerte.

4.2 Formation sur l'équipement cryptographique

Avant d'utiliser de l'équipement cryptographique approuvé par le CST, le gardien de sous-compte COMSEC et le gardien suppléant devraient assister, dans la mesure du possible, à une formation consacrée à cet équipement et approuvée par le CST.

4.2.1 Formation offerte par les fabricants

Certains fabricants d'équipement cryptographique approuvé par le CST offrent de la formation sur leurs produits. Pour suivre ces cours, il faut avoir obtenu un permis de visite auprès du PSI dans les cas où un contrat a été conclu. Si la formation exige un accès au MCC, les Services à la clientèle en matière de COMSEC doivent fournir une autorisation d'accès COMSEC (voir la section 8.5).

4.3 Formation des titulaires de prêts

Les gardiens de sous-compte COMSEC sont habituellement responsables de la formation des titulaires de prêts. Ces derniers sont toutefois admissibles au cours officiel de gardien COMSEC et à celui sur l'équipement cryptographique offerts par le CST, lorsqu'il reste des places.

5 Gestion des sous-comptes COMSEC

5.1 Établissement d'un sous-compte COMSEC

5.1.1 Généralités

Une entreprise du secteur privé doit établir un sous-compte COMSEC avant d'être autorisée à recevoir du MCC.

Dès lors que les Services à la clientèle en matière de COMSEC ont donné leur autorisation, le CCIC est responsable de coordonner l'établissement et la gestion du sous-compte COMSEC de l'entreprise du secteur privé canadien. Un représentant du CCIC doit inspecter le site du sous-compte COMSEC de l'entreprise avant d'autoriser la remise de MCC (voir la section 9.2).

En règle générale, un seul sous-compte COMSEC est établi pour chaque entreprise du secteur privé. Toutefois, lorsque la situation s'y prête, les Services à la clientèle en matière de COMSEC peuvent approuver l'établissement de sous-comptes COMSEC additionnels au sein d'une même entreprise.

Le personnel du sous-compte COMSEC doit compter au minimum les éléments suivants :

- un ASE;
- un gardien de sous-compte COMSEC;
- un gardien suppléant.

NOTA : Dans le cas des sous-comptes COMSEC nécessitant des contrôles d'intégrité par deux personnes (TPI pour *Two-Person Integrity*) ou comptant des zones « jamais seul » (NLZ pour *No-Lone Zone*) (voir respectivement les sections 8.3 et 8.4), il faut nommer plus d'un gardien suppléant de sous-compte COMSEC.

Avant que les Services à la clientèle en matière de COMSEC puissent autoriser l'établissement d'un sous-compte COMSEC et remettre du MCC à une entreprise du secteur privé, celle-ci doit compter les éléments suivants :

- un accord de parrainage avec un parrain autorisé du GC;
- une ECMCC en règle;
- une évaluation PCIE (voir la section 1.11.1);
- une ASI approuvée par SPAC, ainsi que des inspections liées à l'ADR, aux TI et, s'il y a lieu, à la production (seulement pour les cas où des contrats du GC ou étrangers ont été obtenus par l'entremise de SPAC);
- une confirmation de l'inscription au PMC;
- un gardien de sous-compte COMSEC et un gardien suppléant nommés par l'ASE (voir la section 3);
- une ASI approuvée par le CST, ainsi que des inspections équivalentes aux inspections liées à l'ADR et aux TI, comme l'exige le CST (seulement dans le cas d'entreprises du secteur privé qui ne sont pas liées au GC par un contrat conclu par l'entremise de SPAC);
- la documentation requise (p. ex. concept d'opération [CONOP], PSMC, ISP, plans liés au matériel IP) jugée nécessaire par les Services à la clientèle en matière de COMSEC;
- un PA avec le parrain du GC concernant l'approvisionnement de MCC (moins l'équipement cryptographique comptable) (seulement lorsque l'exigent les Services à la clientèle en matière de COMSEC).

5.1.2 Documentation

Les documents suivants doivent être présentés au CCIC :

- une ECMCC et toute entente connexe faisant état du soutien requis pour le MCC;
- un formulaire d'inscription d'un sous-compte rempli;
- un *certificat de nomination* de gardien de sous-compte COMSEC ou de gardien suppléant pour chaque personne nommée;
- les adresses postale et de livraison complètes du sous-compte COMSEC, y compris le numéro de téléphone, l'adresse électronique et le numéro de télécopieur du gardien de sous-compte COMSEC et des gardiens suppléants qui ont été nommés;
- les personnes-ressources après les heures normales de travail, le cas échéant.

5.1.3 Inscription des titulaires de prêts

Le gardien de sous-compte COMSEC doit inscrire les titulaires de prêts avant d'autoriser l'accès au MCC ou son utilisation. En plus des critères énoncés à la section 3.2, l'inscription doit indiquer le nom complet, le titre ou l'indicatif de son poste, le lieu de travail et le numéro de téléphone du titulaire de prêts. Les gardiens de sous-compte COMSEC doivent assurer le suivi local des inscriptions de titulaires de prêts.

5.2 Dossiers et documents

5.2.1 Dossiers d'administration

Le gardien de sous-compte COMSEC doit créer et tenir des dossiers d'administration (manuels [papier] ou électroniques) appropriés pour le système de comptabilité utilisé. Ces dossiers doivent être approuvés par le CCIC et comprendre ce qui suit :

- les récépissés d'expédition par messagerie et par courrier postal ainsi que les récépissés de livraison;
- la correspondance générale;
- les alertes en matière de sécurité des TI (ITSA pour *IT Security Alert*);
- les documents de formation (notamment les certificats de formation du personnel, des titulaires de prêts et des utilisateurs autorisés);
- les bulletins en matière de sécurité des TI (ITSB pour *IT Security Bulletin*);
- les rapports d'incident COMSEC;
- les registres de numéros de transaction.
- le formulaire *Pouvoir de signature COMSEC*;
- les certificats de nomination;
- les attestations d'initiation COMSEC;
- les ECMCC;
- le *Journal de contrôle du matériel COMSEC*;
- les rapports de vérification et les attestations des mesures prises;
- les certificats d'enquête de sécurité;

5.2.2 Dossiers comptables

Le gardien de sous-compte COMSEC doit créer et tenir des dossiers comptables (manuels [papier] ou électroniques) appropriés pour le système de comptabilité utilisé. Ces dossiers doivent être approuvés par le CCIC et comprendre ce qui suit :

- un exemplaire des rapports (voir la section 7), des enregistrements, des registres et des journaux comptables comportant les signatures physiques ou numériques appropriées;
- un exemplaire des rapports d'inventaire (GC-223) (voir la section 7).

5.2.3 Sous-systèmes de comptabilité approuvés

Le CST a approuvé l'emploi de plusieurs systèmes manuels et automatisés de gestion et de comptabilité pour répondre aux exigences de sécurité minimales du SNCMC. Ces systèmes utilisent une terminologie et des procédures assez différentes les unes des autres.

Tous les systèmes prenant en charge le SNCMC doivent être classifiés au niveau PROTÉGÉ A et comporter une classification additionnelle permettant de répondre aux besoins spéciaux en matière d'inventaire et de protéger l'information classifiée stockée dans le système.

NOTA : Les systèmes automatisés de gestion et de comptabilité doivent utiliser les procédures de sauvegarde des données et des systèmes pour atténuer les répercussions des défaillances système.

Prière de communiquer avec le CCIC pour obtenir la liste des systèmes manuels et automatisés approuvés par le CST ou pour demander l'approbation d'un nouveau système.

5.2.4 Classification des documents et des dossiers

Les documents et dossiers du sous-compte COMSEC doivent porter la mention PROTÉGÉ A à moins qu'ils ne contiennent l'un ou l'autre des éléments suivants :

- des renseignements classifiés (p. ex. dates d'entrée en vigueur, titres au long ou remarques classifiés) – dans ce cas, le document ou le dossier doit être marqué en fonction de la sensibilité du contenu;
- une liste de matériel COMSEC provenant d'une source du Royaume-Uni (R.-U.) – dans ce cas, la liste doit être classifiée à tout le moins selon la norme minimale du R.-U., concernant le traitement de ce matériel.

NOTA : Prière de communiquer avec le CCIC pour obtenir de l'aide concernant les règles de classification des dossiers, des documents et des rapports.

5.2.5 Conservation et disposition des documents ainsi que des dossiers

Exception faite des indications du tableau 2 ci-après, le gardien de sous-compte COMSEC (ou l'ASE) doit conserver tous les documents et dossiers inactifs ou archivés du sous-compte COMSEC pendant une période minimale de cinq ans, après quoi le CCIC peut en autoriser la destruction ou demander qu'on les lui achemine aux fins de conservation.

Tableau 2 – Dossiers administratifs et exigences de conservation

Type de dossier	Exigences de conservation
ITSA	Les conserver jusqu'à ce que les Services à la clientèle en matière de COMSEC les remplacent
ITSB	Les conserver jusqu'à ce que les Services à la clientèle en matière de COMSEC les remplacent
Registre de contrôle du matériel COMSEC – Dossiers inactifs	Voir la section 7.1.1
Journal de contrôle du matériel COMSEC	Voir la section 7.2
Attestations d'initiation COMSEC	Voir la section 8.2.2
Registres des visiteurs	Voir la section 9.1.3

5.2.6 Registre de contrôle du matériel COMSEC

Le *Registre de contrôle du matériel COMSEC* doit être marqué « PROTÉGÉ A », sauf dans le cas des exigences suivantes :

- **Titres au long classifiés ou protégés :** un *Registre de contrôle du matériel COMSEC* qui contient des titres au long classifiés ou protégés doit être classifié ou protégé au niveau de sensibilité le plus élevé des titres concernés.
- **Clés :** un *Registre de contrôle du matériel COMSEC* qui contient des titres abrégés ou des titres au long non classifiés, y compris les dates d'entrée en vigueur des clés, doit être classifié au minimum au niveau CONFIDENTIEL.

- **Matériel assujetti aux contrôles TPI et NLZ :** un *Registre de contrôle du matériel COMSEC* (électronique ou manuel) qui contient des titres abrégés ou des titres au long non classifiés pour du matériel assujetti à un contrôle TPI ou NLZ doit être classifié au minimum au niveau CONFIDENTIEL.

5.2.7 Accès aux documents et aux dossiers

Le gardien de sous-compte COMSEC doit limiter l'accès aux documents et aux dossiers du sous-compte COMSEC aux personnes qui répondent au principe du besoin de connaître et aux exigences d'accès au matériel COMSEC, et qui possèdent l'habilitation de sécurité appropriée.

5.3 Changements à un sous-compte COMSEC

5.3.1 Changement de gardien de sous-compte COMSEC ou de gardien suppléant

Avant le départ du gardien de sous-compte COMSEC ou du gardien suppléant inscrit, l'ASE doit fournir au CCIC un *certificat de nomination* pour le nouveau gardien de sous-compte ou gardien suppléant, en veillant à fournir les informations suivantes :

- les renseignements personnels sur la personne nouvellement nommée;
- la section « Cessation des fonctions » remplie pour la personne qui sera remplacée.

NOTA 1 : L'ASE doit s'assurer que la personne nouvellement nommée répond à toutes les exigences de nomination pour le poste concerné et qu'elle a reçu la formation de gardien COMSEC ainsi qu'une attestation d'initiation COMSEC.

NOTA 2 : Pour connaître les exigences relatives aux départs inexpliqués, y compris les départs permanents, voir la section 5.4.5.

5.3.1.1 Planification d'un remplacement de gardien de sous-compte COMSEC

Le remplacement du gardien de sous-compte COMSEC sortant devrait être planifié au moins 90 jours civils avant la date de son départ.

5.3.1.2 Prise d'inventaire au moment du remplacement

Une fois que le CCIC a approuvé la nomination du nouveau gardien de sous-compte COMSEC, les gardiens entrant et sortant doivent s'acquitter des tâches suivantes :

- effectuer un inventaire physique (visuel) de tout le MCC détenu au sous-compte COMSEC – le remplacement du gardien de sous-compte COMSEC entre en vigueur à la date de signature du *Rapport d'inventaire* (GC-223);
- préparer un *Rapport de matériel COMSEC* (GC-223) de tout le MCC qui sera transféré au nouveau gardien, indiquer dans le bloc 1 du rapport qu'il s'agit d'un « Inventaire » et cocher la case « Inventorié » dans le bloc 14; le rapport doit être transmis du sous-compte COMSEC au CCIC; le nouveau gardien doit apposer sa signature dans le bloc 15 et le gardien sortant, dans le bloc 16 à titre de témoin.

L'original signé (exemplaire n^{o} 1) doit être envoyé au CCIC et un double signé (exemplaire n^{o} 2), versé dans le dossier du sous-compte COMSEC.

NOTA : Le gardien sortant demeure responsable du matériel COMSEC faisant l'objet d'écarts irrésolus jusqu'à ce que le CCIC ait déposé un *rapport de rapprochement d'inventaire* au sous-compte COMSEC.

5.3.2 Changements à une demande de pouvoir de signature de sous-compte COMSEC

Le formulaire *Demande de pouvoir de signature COMSEC* est un formulaire **local** appelé à circuler entre un sous-compte COMSEC et **ses installations locales d'expédition-réception**. Il doit être signé par l'ACM ou l'ACO et doit contenir le nom, le numéro de téléphone et la signature des membres du personnel du compte COMSEC et de tout autre employé du ministère autorisé à signer un accusé de réception pour les colis contenant du MCC. Le formulaire rempli doit être conservé dans le répertoire chronologique du sous-compte COMSEC.

5.3.3 Changements à l'information d'inscription du sous-compte COMSEC

Le gardien de sous-compte COMSEC doit présenter au CCIC, dans les meilleurs délais, tout changement à l'information d'inscription du sous-compte COMSEC (p. ex. adresses postale et de livraison, numéros de téléphone). Ces changements doivent être présentés dans le formulaire *Inscription d'un sous-compte*.

5.3.4 Changement du niveau de classification d'un sous-compte COMSEC

Lorsqu'il faut changer le niveau de classification d'un sous-compte COMSEC, l'ASE doit présenter une demande écrite à l'autorité contractante (généralement le parrain du GC). L'autorité contractante présente ensuite une LVERS modifiée au personnel du PSI, qui doit ensuite demander aux Services à la clientèle en matière de COMSEC une autorisation pour élever ou abaisser le niveau de classification du sous-compte. La demande doit inclure une justification du besoin (p. ex. des changements aux exigences du contrat) et indiquer le nouveau niveau de classification demandé.

Si aucun contrat du GC n'est visé, l'ASE de l'entreprise du secteur privé doit présenter la demande de changement à son parrain du GC. Celui-ci présente ensuite la demande aux Services à la clientèle en matière de COMSEC.

NOTA : L'ASI ainsi que les exigences des inspections liées à l'ADR, aux TI et à la production, ou encore leur équivalent, doivent être examinées par l'autorité concernée, le cas échéant.

5.4 Absence du personnel de garde COMSEC

5.4.1 Absence temporaire du gardien de sous-compte COMSEC

Lorsque le gardien de sous-compte COMSEC s'absente pour une période d'au plus 60 jours civils, l'ASE doit veiller à ce que le gardien suppléant assume les responsabilités et les fonctions du gardien de sous-compte COMSEC.

5.4.2 Retour du gardien de sous-compte COMSEC

Au retour du gardien de sous-compte COMSEC après une absence temporaire, le gardien suppléant de sous-compte COMSEC doit l'informer de tous les changements apportés au compte durant son absence.

Lorsque du MCC a été reçu et que le gardien suppléant a signé un *accusé de réception* (GC-223) ou un *rapport de possession* (GC-223), le gardien de sous-compte COMSEC doit faire l'inventaire du MCC. Il doit ensuite contresigner et dater le devant de l'exemplaire du rapport du sous-compte COMSEC, et y inscrire la remarque « reçu du gardien suppléant de sous-compte COMSEC ». Le gardien suppléant est dès lors relevé de toute responsabilité ultérieure à l'égard du MCC.

Dans les cas où un MCC a été remis par le sous-compte ou détruit, le gardien de sous-compte COMSEC doit rapprocher cette activité en comparant le rapport en question avec le *Registre de contrôle du matériel COMSEC* et annoter la première page du rapport en guise d'attestation.

5.4.3 Absence temporaire du gardien suppléant de sous-compte COMSEC

Lorsque le gardien suppléant de sous-compte COMSEC s'absente pour une période d'au plus 60 jours civils, l'ASE doit veiller à ce que le second gardien suppléant assume les responsabilités et les fonctions du gardien suppléant absent. Si aucun second gardien suppléant n'a été nommé, l'ASE doit en nommer un.

5.4.4 Absence de plus de 60 jours civils

Une absence de plus de 60 jours civils du gardien de sous-compte COMSEC ou du gardien suppléant doit être traitée comme une absence permanente, et l'ASE doit nommer un nouveau gardien de sous-compte COMSEC ou un nouveau gardien suppléant, le cas échéant.

5.4.5 Départ inexpliqué du gardien de sous-compte COMSEC ou du gardien suppléant

Advenant le départ inexpliqué (autre qu'un décès, une maladie grave ou un transfert de personnel à court préavis), soudain, définitif ou permanent du gardien de sous-compte COMSEC ou du gardien suppléant, l'ASE doit suivre la procédure suivante :

1. signaler immédiatement les circonstances du départ au CCIC;
2. nommer un nouveau gardien de sous-compte COMSEC ou un nouveau gardien suppléant, selon le cas;
3. faire changer les mots de passe concernés de même que les combinaisons ou les clés des contenants et des chambres fortes;
4. veiller à ce que le nouveau gardien de sous-compte COMSEC ou gardien suppléant mène immédiatement l'inventaire du compte avec un témoin ayant l'habilitation de sécurité appropriée (voir la section 2.6.8);
5. s'assurer qu'un représentant ou un vérificateur désigné par le CCIC effectue une vérification du sous-compte COMSEC.

5.5 Fermeture d'un sous-compte COMSEC

5.5.1 Demande de fermeture d'un sous-compte COMSEC

Lorsqu'un sous-compte COMSEC n'a plus besoin de détenir de MCC (p. ex. à la fin d'un contrat qui exige du MCC), l'ASE doit s'adresser par écrit au CCIC pour demander que les Services à la clientèle en matière de COMSEC ferment ledit sous-compte COMSEC. Les Services à la clientèle en matière de COMSEC coordonnent toutes les demandes de fermeture de sous-compte COMSEC avec les organismes parrains, le cas échéant.

Une fois que les Services à la clientèle en matière de COMSEC ont autorisé la fermeture du sous-compte COMSEC, l'ASE doit s'acquitter des tâches suivantes :

- demander au gardien de sous-compte COMSEC de retourner tout le MCC au CCIC;
- fournir au CCIC un certificat de cessation des fonctions (voir le bloc D du certificat de nomination) pour chaque membre du personnel du sous-compte COMSEC;

- retourner tous les dossiers du sous-compte au CCIC (à la réception de la confirmation par le CCIC de la fermeture du sous-compte COMSEC).

5.5.2 Fermeture exigée par le CST

Dans certaines circonstances exceptionnelles (p. ex. omission d'appliquer les procédures COMSEC appropriées ou d'assurer une sécurité physique adéquate, vente ou faillite de l'entreprise, ou annulation d'un contrat), le CST peut fermer un sous-compte COMSEC. Dans un tel cas, l'intention de fermer le compte est signifiée par écrit à l'entreprise concernée.

5.5.3 Conditions préalables à la fermeture

Le CCIC ne peut fermer un sous-compte COMSEC que lorsque les étapes suivantes ont été mises en œuvre :

1. tout le MCC a été retourné au CCIC, et le solde du sous-compte COMSEC devient nul;
2. l'ASE a transmis au CCIC les *certificats de cessation des fonctions* du personnel de garde COMSEC (voir le bloc D du *Certificat de nomination*), ainsi que tous les documents du sous-compte COMSEC.

5.5.4 Confirmation de la fermeture

Lorsque le CCIC a confirmé que les conditions préalables à la fermeture ont été satisfaites, l'ASE est informé que le sous-compte COMSEC a été fermé et que le personnel de garde du sous-compte COMSEC a été relevé des fonctions le liant audit sous-compte. Jusqu'à ce qu'ils aient reçu un avis officiel du CCIC, le gardien de sous-compte COMSEC et le gardien suppléant demeurent responsables du sous-compte et de tout écart concernant le MCC en question.

5.6 Maintien d'un sous-compte COMSEC dont le solde est nul

Un sous-compte COMSEC qui ne détient aucun MCC est appelé un sous-compte COMSEC à solde nul. Une demande de maintien de ce type de sous-compte doit être présentée aux Services à la clientèle en matière de COMSEC, par l'entremise du CCIC, et justifiée (p. ex. nouveau contrat ou prolongation de contrat). Les Services à la clientèle en matière de COMSEC coordonnent, avec les organismes parrains s'il y a lieu, toutes les demandes de maintien d'un sous-compte COMSEC dont le solde est nul.

5.7 Suspension d'un sous-compte COMSEC

5.7.1 Généralités

Le CCIC peut suspendre temporairement un sous-compte COMSEC (voir la section 1.8) lorsqu'une infraction a été commise ou lorsque le sous-compte n'a pas été géré tel qu'il est exigé. Un sous-compte COMSEC peut également être suspendu advenant l'un ou l'autre des cas de figure suivants :

- l'ASE ne prend pas les mesures nécessaires pour corriger les lacunes graves signalées dans le Rapport de vérification du sous-compte COMSEC ou ne remet pas une attestation des mesures prises indiquant que des mesures correctives sont mises en œuvre;
- le nombre d'infractions à la sécurité ou les pratiques de gestion et de rapports au sous-compte COMSEC démontrent la non-observation des politiques et des procédures COMSEC.

NOTA : Toute suspension, peu importe sa durée, peut avoir des conséquences graves sur les activités du sous-compte COMSEC.

5.7.2 Conséquence d'une suspension

Le CCIC cessera de remettre du MCC à un sous-compte COMSEC suspendu. Le personnel de garde demeurera en poste pour effectuer les autres activités normales du compte, y compris les mesures correctives qui pourraient mener à la levée de la suspension.

NOTA : Le CCIC informera la Direction de la sécurité industrielle canadienne (DSIC) de SPAC, l'ASE, le parrain du GC et le gardien de sous-compte COMSEC de la suspension de toute remise de MCC au sous-compte concerné. L'avis inclura la liste des écarts ayant donné lieu à la suspension, les mesures correctives à prendre pour que la suspension soit levée, de même qu'un échéancier.

5.7.3 Levée d'une suspension

Le CCIC peut lever la suspension après avoir reçu l'*Attestation des mesures prises* confirmant que les mesures correctives ont été prises (ou sont en voie de l'être). Avant de lever la suspension, le CCIC ou encore un représentant ou vérificateur désigné par le CCIC mènera une nouvelle vérification du compte pour s'assurer que les lacunes ont été corrigées.

Une fois la suspension levée, le CCIC informera la DSIC, l'ASE, le parrain du GC et le gardien de sous-compte COMSEC que du MCC pourra de nouveau être remis au sous-compte concerné.

6 Désignation du matériel COMSEC comptable

6.1 Généralités

Le MCC est du matériel COMSEC qui nécessite, au titre du SNCMC, un contrôle et une comptabilité correspondant à son code de comptabilité (CC) et dont le transfert ou la divulgation risquerait de porter préjudice à la sécurité nationale du Canada et de ses alliés.

6.2 Désignation

6.2.1 Titre au long

Le titre au long fournit une description générale du MCC. Il est attribué à un MCC à son point d'origine ou au CST. Les titres au long sont généralement NON CLASSIFIÉ, mais il y a des exceptions.

6.2.2 Titre abrégé

Un titre abrégé est attribué à un MCC à son point d'origine ou au CST aux fins de comptabilité. Il consiste en une combinaison de lettres et de chiffres d'un maximum de 24 caractères. Certains systèmes automatisés de gestion et de comptabilité approuvés par le CST (p. ex. le Système de gestion électronique des clés [EKMS pour *Electronic Key Management System*] du GC) n'acceptent pas les caractères spéciaux (p. ex. /, -, * ou #). Pour ces systèmes, les caractères spéciaux qui pourraient figurer dans les titres abrégés du MCC (notamment les plaques signalétiques d'équipement cryptographique et les publications COMSEC) sont remplacés par une espace. Les titres abrégés sont NON CLASSIFIÉ.

6.2.3 Édition

Le MCC peut être désigné par un indicatif d'édition alphabétique ou numérique unique (p. ex. A, AA, B). Les éditions de MCC ont généralement une durée limitée et sont remplacées dès l'entrée en vigueur de l'édition suivante.

6.2.4 Numéros de comptabilité

6.2.4.1 Attribution des numéros de comptabilité

Un numéro de registre ou de série comptable unique (p. ex. 1234, Reg. 103) peut être attribué au MCC à son point d'origine pour en faciliter la comptabilité. Le numéro de série est utilisé avec les articles cryptographiques contrôlés (CCI) ou l'équipement cryptographique, tandis que le numéro de registre est utilisé pour tout autre matériel nécessitant un numéro de comptabilité.

6.2.5 Code de comptabilité

6.2.5.1 Description

Un CC est un code numérique attribué au point d'origine du MCC pour indiquer ses exigences en matière de comptabilité et de rapports. Le CC figure sur tous les *rapports de matériel COMSEC*, mais n'apparaît normalement pas sur le MCC lui-même. Le CC attribué à l'origine ne doit pas être changé sans l'autorisation du CCIC, lequel doit demander l'autorisation du point d'origine (par les voies COMSEC).

NOTA 1 : En cas de doutes sur la comptabilité du matériel COMSEC, prière de communiquer avec le CCIC.

NOTA 2 : Les CC 3 et 5 ne sont pas utilisés.

6.2.5.2 Code de comptabilité 1

Le CC 1 est attribué au MCC physique et électronique faisant l'objet d'une comptabilité continue de la part du NCOR en fonction d'un numéro de série et/ou d'un numéro de registre figurant dans le SNCMC. Le MCC portant le CC 1 comprend :

- certaines clés physiques non classifiées et toutes les clés physiques classifiées portant la mention CRYPTO;
- tout l'équipement cryptographique (y compris les CCI) approuvé pour le traitement classifié;
- les logiciels et micrologiciels cryptographiques classifiés qui équivalent fonctionnellement aux opérations et à la cryptographie de l'équipement cryptographique ou qui les émulent;
- les manuels classifiés de maintenance complète et de maintenance au dépôt (ainsi que leurs modificatifs imprimés) qui contiennent de l'information cryptographique.

6.2.5.3 Code de comptabilité 2

Le CC 2 est attribué au MCC physique faisant l'objet d'une comptabilité continue par quantité au NCOR dans le SNCMC. Le MCC portant le CC 2 comprend :

- les composants classifiés et les composants de CCI (p. ex. ensembles modulaires, cartes équipées logiques [PWA pour *Printed Wiring Assembly*], circuits intégrés [CI], microcircuits, puces, permutateurs) qui sont destinés à être installés (mais qui ne le sont pas encore) dans l'équipement cryptographique (voir l'ITSD-08);
- des dispositifs COMSEC précis;
- les publications COMSEC.

6.2.5.4 Code de comptabilité 4

Le CC 4 est attribué au MCC physique ainsi qu'aux clés traditionnelles en format électronique qui, après réception initiale, font l'objet d'une comptabilité locale, en fonction d'un numéro de série ou d'un numéro de registre, au compte COMSEC responsable, au sein du SNCMC. Le MCC portant le CC 4 peut inclure les éléments suivants :

- les publications COMSEC non classifiées ou classifiées traitant d'un sujet cryptographique (p. ex. manuels de maintenance classifiés);
- les clés protégées et non classifiées (p. ex. clés de formation, de test et de maintenance);
- tout autre matériel COMSEC non classifié ou classifié qui, en raison de la nature de l'information COMSEC qu'il contient, doit être comptabilisé dans le SNCMC.

NOTA : Le MCC portant le CC 4 est comptabilisé seulement au compte COMSEC, et non au NCOR.

6.2.5.5 Code de comptabilité 6

Le CC 6 est attribué aux clés électroniques qui, en fonction d'un numéro de registre, font l'objet d'une comptabilité continue du NCOR au sein du SNCMC. Le CC 6 peut être attribué aux clés électroniques qui se caractérisent comme suit :

- doivent protéger de l'information ayant une utilité à long terme sur le plan du renseignement (p. ex. TRÈS SECRET);
- servent à protéger d'autres clés (p. ex. clés de chiffrement de clés [KEK pour *Key Encryption Key*]);
- sont utilisées aux fins d'interopérabilité conjointe ou combinée;
- portent la mention CRYPTO;
- servent à produire d'autres clés électroniques (p. ex. clés de production de clés);
- sont produites à partir d'une clé physique CC 1.

6.2.5.6 Code de comptabilité 7

Le CC 7 est attribué aux clés électroniques qui, après réception initiale, font l'objet d'une comptabilité locale en fonction d'un numéro de registre attribué au compte COMSEC responsable dans le SNCMC.

6.3 Inscription du matériel COMSEC dans le Système national de contrôle du matériel COMSEC

Un MCC doit être inscrit dans le SNCMC dès qu'un CC lui a été attribué. Ce MCC doit être contrôlé dans le SNCMC jusqu'à ce que sa destruction ou toute autre forme de disposition soit autorisée, ou jusqu'à ce que l'autorité compétente retire l'exigence de comptabilité. Un *rapport de matériel COMSEC* est utilisé pour inscrire le matériel COMSEC dans le SNCMC, tel qu'il est décrit à la section 7.4.

6.4 Types de matériel COMSEC comptable

La comptabilité dans le SNCMC est approuvée pour les trois types de MCC suivants :

- clés cryptographiques;
- équipement cryptographique;
- publications COMSEC.

6.4.1 Clés cryptographiques

Le terme « clé » (également appelé « matériel de chiffrement » dans d'autres documents) se définit comme étant de l'information utilisée pour établir et changer périodiquement les opérations accomplies dans un équipement cryptographique, ce qui a pour effet de chiffrer et déchiffrer des signaux électroniques et des signatures numériques, de déterminer des modèles de contremesures électroniques ou de produire d'autres clés. La clé est normalement comptabilisée au moyen de son titre abrégé.

NOTA : Tel qu'il est mentionné à la section 2.2.3, le terme « clé » est utilisé dans l'ensemble du document (sauf dans le glossaire) pour recouvrir la notion de « clé cryptographique ».

6.4.2 Équipement cryptographique

L'équipement cryptographique (dont les CCI) est généralement désigné et comptabilisé selon son titre abrégé, son titre au long et son numéro de série plutôt qu'au moyen de ses composants ou sous-ensembles. Chaque fois qu'un composant ou qu'un sous-ensemble auquel a été attribué un CC est retiré de l'équipement hôte, ce composant ou sous-ensemble doit être comptabilisé dans le SNCMC et doit être désigné séparément par son titre abrégé individuel. Pour de plus amples renseignements sur un équipement cryptographique particulier, prière de consulter le document approprié de la série des doctrines canadiennes en matière de cryptographie (CCD pour *Canadian Cryptographic Doctrine*).

NOTA : Il est possible que ces détails ne s'appliquent pas toujours à la comptabilité du matériel IP (voir l'ITSD-08).

6.4.3 Article cryptographique contrôlé

La mention CCI (*Controlled Cryptographic Item*) indique un type d'équipement cryptographique qui doit toujours être comptabilisé et contrôlé dans le SNCMC. Le terme « CCI » s'applique à de l'équipement sécurisé et non classifié de communications et de traitement de l'information particulier ainsi qu'aux composants et ensembles cryptographiques connexes.

Dans de nombreux cas, un CCI ne recevra pas de titre abrégé, mais portera plutôt une désignation commerciale du fabricant. Cet équipement portera la mention « article cryptographique contrôlé » ou « CCI », ainsi qu'une étiquette sur laquelle figurera un numéro de série du gouvernement.

Comme les CCI et leurs composants cryptographiques connexes utilisent une logique cryptographique classifiée, seuls le matériel informatique ou les micrologiciels renfermant cette logique sont non classifiés. Les dessins techniques cryptographiques, les descriptions logiques, le principe de fonctionnement, les programmes informatiques et l'information cryptographique connexes demeurent classifiés.

6.4.4 Publications

Les publications peuvent inclure ce qui suit :

- des manuels de maintenance cryptographique;
- des pages sensibles d'un manuel de maintenance cryptographique;
- des instructions d'exploitation du matériel cryptographique;
- des manuels classifiés de maintenance intégrale;
- des manuels classifiés de maintenance au dépôt;
- des descriptions de logiques cryptographiques;
- des schémas de logiques cryptographiques;
- des spécifications décrivant une logique cryptographique;
- d'autres publications opérationnelles cryptographiques et non cryptographiques classifiées;
- des pages de remplacement pour les publications mentionnées ci-dessus et des publications semblables;
- des extraits de publications COMSEC comptables, ou des suppléments et des addendas à ces publications.

6.5 Mentions spéciales et mises en garde

6.5.1 CRYPTO

La mention « CRYPTO » sert à indiquer la sensibilité particulière du MCC sur lequel elle figure (ou est autrement désignée). Les articles qui portent cette mention ou qui sont désignés comme tels par le CST doivent toujours être comptabilisés au sein du SNCMC. La mention CRYPTO est apposée en caractères gras sur les cartes de circuit imprimé, sur le dessus des clés imprimées, sur les cédéroms, sur les diverses variables de clés et, au besoin, sur l'équipement ainsi que sur les étiquettes ou plaques d'identification apposées aux dispositifs de stockage physiques (p. ex. dispositifs de stockage de clés [KSD-64]) contenant des clés électroniques.

6.5.2 Réservé ou « Eyes Only »

L'accès au matériel COMSEC qui porte la mise en garde « Eyes Only » (p. ex. CAN/EYES ONLY, CAN/US/EYES ONLY, CAN/UK/EYES ONLY) est réservé exclusivement aux nations dont le nom figure dans la mise en garde. L'accès doit répondre aux exigences de contrôle d'accès du MCC dont la liste figure à la section 8.

6.6 Matériel COMSEC non comptable

Le matériel COMSEC connexe, notamment la correspondance, les journaux et les rapports, peut être catégorisé comme étant du matériel COMSEC non comptable. Les documents contenant du matériel COMSEC classifié, mais ne portant aucun CC sont également inclus dans cette catégorie. Ce matériel doit être traité par les voies COMSEC, mais est exclu de la comptabilité dans le SNCMC. Il peut arriver que le CCIC requière que le matériel COMSEC non comptable fasse l'objet d'un suivi local.

7 Registres, formulaires, rapports et avis comptables

7.1 Registre de contrôle du matériel COMSEC

Le *Registre de contrôle du matériel COMSEC* est le principal outil comptable d'un sous-compte COMSEC d'une entreprise du secteur privé qui n'utilise pas d'outil comptable automatisé. Il permet de comptabiliser et de faire le suivi de tout le MCC produit ou reçu par le sous-compte COMSEC, de sa production ou de sa réception jusqu'à sa disposition définitive. Le registre est composé de feuilles de registre individuelles (une par titre abrégé) pour tout le MCC détenu en stock par le sous-compte COMSEC. Le registre sert également à enregistrer les prêts accordés aux titulaires de prêts (au moyen d'accusés de réception).

Le registre compte sept sections :

- section 1 : contient tous les articles CC 1, moins l'équipement;
- section 2 : contient tous les articles CC 2, moins l'équipement;
- section 3 : non utilisée;
- section 4 : contient tous les articles CC 4, moins l'équipement;
- section 5 : contient l'équipement cryptographique CC 1, 2, et 4, y compris les CCI;
- section 6 : contient les CIK faisant l'objet d'un suivi local (en dehors du SNCMC);
- section 7 : contient les dossiers inactifs.

NOTA : Il ne faut rien inscrire dans le *Registre de contrôle du matériel COMSEC* lorsqu'il s'agit de remettre du MCC aux utilisateurs autorisés, puisque le *Journal de contrôle du matériel COMSEC* (voir la section 7.2) est déjà prévu à cette fin.

7.1.1 Dossiers inactifs

La section 7 du *Registre de contrôle du matériel COMSEC* sert à conserver les feuilles de registre inactives extraites des autres sections. Ces feuilles de registre sont insérées dans la section 7 par ordre chronologique, selon la date de disposition définitive inscrite sur chaque feuille. Les dossiers inactifs doivent être conservés jusqu'à ce que la destruction des feuilles de registre soit autorisée. L'autorisation de destruction est donnée dans le *Rapport de rapprochement d'inventaire COMSEC* après chaque inventaire annuel du matériel détenu par un sous-compte. Le CCIC doit autoriser la destruction des feuilles de registre dont la date précède de 12 mois ou plus la date de prise d'inventaire.

7.2 Journal de contrôle du matériel COMSEC

Le *Journal de contrôle du matériel COMSEC* sert à enregistrer l'accès des utilisateurs autorisés (voir la section 2.6.7) au MCC d'un sous-compte COMSEC. Chaque feuille de journal doit être conservée jusqu'à ce que sa destruction soit autorisée. Cette autorisation repose sur les *rapports de rapprochement d'inventaire COMSEC*, comme c'est le cas pour le *Registre de contrôle du matériel COMSEC*.

Le *Journal de contrôle du matériel COMSEC* doit être rempli tel qu'il est énoncé dans le tableau 3 ci-après.

Tout MCC auquel accède un utilisateur autorisé doit être retourné au gardien de sous-compte COMSEC, au gardien suppléant ou au titulaire de prêts avant la fin de la journée ouvrable pour laquelle l'autorisation d'accès a été accordée.

Tableau 3 – Rédaction du *Journal de contrôle du matériel COMSEC*

Colonne	Entrée
1	Date d'accès au MCC ou de prêt du MCC.
2	Heure d'accès au MCC ou de prêt du MCC.
3	Titre abrégé, édition et, le cas échéant, numéro de comptabilité du MCC.
4	Signature de l'utilisateur autorisé; par sa signature, celui-ci s'engage à protéger le MCC en sa possession.
5	Signature du gardien de sous-compte COMSEC, du gardien suppléant ou du titulaire de prêts au moment de l'accès au MCC ou du prêt du MCC.
6	Heure de retour du MCC ou de l'annulation de l'accès.
7	Signature du gardien de sous-compte COMSEC, du gardien suppléant ou du titulaire de prêts au moment du retour du MCC ou de l'annulation de l'accès.

7.3 Dossiers et registres comptables locaux

7.3.1 Généralités

Les dossiers et registres comptables locaux peuvent servir à gérer le contrôle et la distribution du MCC.

NOTA : Il ne faut pas confondre les termes « comptabilité locale » et « suivi local », ce dernier étant employé lors de la gestion du matériel COMSEC qui n'est **pas** comptabilisé dans le SNCMC.

7.3.2 Fiche d'instructions de traitement/fiche d'élimination

La *Fiche d'instructions de traitement/fiche d'élimination* (HI/DR pour *Handling Instructions/Disposition Record*) peut servir à inscrire la remise ou la destruction de segments de clé individuels. Avant de remettre une clé, le gardien de sous-compte COMSEC doit entrer le titre abrégé et ses attributs sur la fiche HI/DR. La fiche est NON CLASSIFIÉ, mais devient CONFIDENTIEL dès qu'une entrée y est faite. La personne qui effectue la destruction des segments de clé et le témoin qui assiste à cette destruction doivent tous deux apposer leurs initiales ou leur signature sur la fiche HI/DR, en regard de l'entrée correspondant au segment détruit.

Le gardien de sous-compte COMSEC doit examiner chaque fiche HI/DR pour confirmer la destruction de chaque segment de clé avant d'utiliser l'information pour préparer un *rapport de destruction consolidé* (GC-223).

7.3.3 Registres comptables locaux

Lorsque la distribution ou la redistribution du MCC ne peuvent pas être comptabilisées dans un système automatisé approuvé par le CST, le gardien de sous-compte COMSEC doit établir un système de comptabilité manuel pour contrôler et comptabiliser localement le matériel. Le *Registre de contrôle du matériel COMSEC* peut servir au contrôle local du matériel redistribué.

7.3.4 Journaux des numéros de transaction

Les *rapports de matériel COMSEC* entrants et sortants (p. ex. *rapports de possession*, *rapports de destruction* et *accusés de réception*) doivent comporter des numéros de transaction (blocs 4 et 6). Les numéros de transaction doivent se suivre de façon consécutive (sans sauter de numéro) à compter de la date d'ouverture du sous-compte COMSEC jusqu'à sa date de fermeture.

Il faut utiliser des ensembles de numéros de transaction (entrant et sortant) pour chaque type de rapport (voir le bloc 1 du *Rapport de matériel COMSEC*). Les gardiens de sous-compte COMSEC peuvent concevoir et utiliser toute méthode de suivi qui leur semble adéquate pour assurer le respect des exigences relatives aux numéros de transaction.

7.4 Rapports de matériel COMSEC

Le formulaire *Rapport de matériel COMSEC* polyvalent (appelé également « GC-223 ») est le principal formulaire utilisé pour le contrôle et la comptabilité du MCC. Ce rapport sert à ce qui suit :

- communiquer tout changement dans l'état du MCC (p. ex. remise, possession, dispense de comptabilité ou destruction);
- communiquer de l'information sur les stocks d'un sous-compte COMSEC (p. ex. un *rapport d'inventaire*);
- communiquer une mesure prise relativement à un MCC (p. ex. un *avis de recherche*).

Des instructions générales sur la préparation de différents types de *rapports de matériel COMSEC* sont données au verso du GC-223. Les sections qui suivent portent sur les exigences particulières liées à la préparation et à la distribution de chaque type de rapport.

7.4.1 Rapport de transfert

La distribution d'un MCC entre deux comptes COMSEC primaires s'appelle un « transfert ». Sauf dans le cas d'une transaction de compte de matériel IP (voir l'ITSD-08), le sous-compte COMSEC d'une entreprise du secteur privé doit toujours communiquer avec le CCIC lorsqu'il faut transférer un MCC hors de son sous-compte COMSEC vers un compte primaire autre que le CCIC ou vers un sous-compte COMSEC à l'extérieur de l'entreprise.

7.4.2 Accusé de réception

7.4.2.1 Généralités

La distribution de MCC du CCIC à un sous-compte COMSEC ou encore d'un sous-compte COMSEC à un titulaire de prêts s'appelle une « remise ». La remise de MCC est inscrite dans un *accusé de réception* (GC-223) qui permet d'en assurer le suivi. Le MCC remis peut être expédié sous forme de colis ou livré en mains propres au destinataire. Les colis emballés aux fins d'expédition doivent être préparés conformément aux dispositions stipulées à la section 10.

7.4.2.2 Distribution

Lorsqu'il distribue du MCC à un titulaire de prêts, le gardien de sous-compte COMSEC doit utiliser un *accusé de réception*.

En signant l'*accusé de réception*, le titulaire de prêts atteste qu'il accepte le matériel énuméré et qu'il comprend les exigences en matière de manutention du MCC qui lui est confié. Avant de signer l'*accusé de réception*, le titulaire de prêts doit inspecter le MCC pour vérifier si celui-ci correspond à la description du document et pour en établir l'état (voir la section 10).

Les responsabilités liées au contrôle et au suivi du matériel remis continuent de relever du gardien de sous-compte COMSEC; par conséquent, les exemplaires d'*accusés de réception* pour le matériel remis aux titulaires de prêts ne sont pas envoyés au CCIC.

NOTA : Le gardien de sous-compte COMSEC doit examiner les *accusés de réception* tous les six mois pour vérifier l'exactitude de leur information et établir si les règles concernant le MCC ont été respectées.

7.4.2.3 Responsabilité

La responsabilité à l'égard du MCC remis incombe à la fois au sous-compte COMSEC ayant remis le matériel et au titulaire de prêts. Après avoir signé l'*accusé de réception*, le titulaire de prêts assume la responsabilité pour ce qui a trait au soin et au contrôle de tout le MCC figurant sur le document; la signature du titulaire de prêts sur l'*accusé de réception* ne dégage toutefois pas le gardien de sous-compte COMSEC de sa responsabilité envers le MCC remis.

7.4.2.4 Confirmation avant la remise

Le gardien de sous-compte COMSEC doit s'assurer que le titulaire de prêts auquel il a l'intention de remettre du MCC répond aux exigences stipulées à la section 3.2 et à l'Annexe A, et qu'il se plie aux exigences suivantes :

- disposer des installations d'entreposage requises pour le matériel figurant sur l'*accusé de réception*;
- avoir reçu la formation appropriée concernant la manutention, l'entreposage, l'utilisation et la destruction (lorsqu'elle est autorisée) du MCC figurant sur l'*accusé de réception*;
- être au courant de ce qui constitue un incident COMSEC;
- avoir établi, au besoin, un système de comptabilité locale qui lui permette d'exercer un contrôle rigoureux sur chaque article de MCC figurant sur l'*accusé de réception*, lorsqu'il est nécessaire de permettre à un utilisateur autorisé d'accéder à du MCC (voir la section 2.6.7);
- signer l'*accusé de réception* pour attester la réception du matériel remis et sa compréhension des responsabilités associées à la manutention du MCC figurant sur l'*accusé de réception*.

7.4.2.5 Retour du matériel COMSEC comptable

Un MCC inscrit à un sous-compte COMSEC, mais qui n'est plus requis, doit être retourné au CCIC après avoir rempli un *Rapport de matériel COMSEC* (GC-223).

Au moment de la réception et de la vérification du matériel retourné, le CCIC doit signer le *Rapport de matériel COMSEC* (GC-223) et le retourner au sous-compte COMSEC, dégageant par le fait même le sous-compte COMSEC de sa responsabilité à l'égard du matériel.

Lorsqu'ils n'en ont plus besoin, les titulaires de prêts doivent retourner le MCC au gardien de sous-compte COMSEC, sauf si celui-ci en a autorisé la destruction locale. Le gardien doit préparer un *accusé de réception* pour le matériel retourné par un titulaire de prêts. Il doit s'assurer que l'*accusé de réception*, qui énumère le matériel retourné par le titulaire de prêts, est adressé au sous-compte COMSEC. En signant l'*accusé de réception*, le gardien de sous-compte COMSEC dégage le titulaire de prêts de sa responsabilité à l'égard du MCC retourné.

7.4.3 Rapport de possession

7.4.3.1 Généralités

Des circonstances peuvent parfois exiger qu'un sous-compte COMSEC prenne en charge un MCC pour lequel il n'existe aucun enregistrement comptable dans le SNCMC.

Le *Rapport de possession* (GC-223) sert à consigner l'inscription d'un MCC dans le SNCMC dans les circonstances suivantes :

- lorsqu'un MCC en cours de développement ou de fabrication a été accepté par le GC (voir l'ITSD-08) après avoir été reçu sans *accusé de réception* correspondant;
- lorsqu'un MCC déclaré perdu et retiré de la comptabilité est retrouvé;
- lorsqu'une publication COMSEC comptable nécessitant un contrôle en vertu du SNCMC est reproduite (avec l'autorisation du CCIC seulement) en totalité ou en partie;
- lorsqu'un support magnétique ou optique est utilisé pour remettre une clé électronique;
- lorsqu'un sous-compte COMSEC non automatisé enregistre son inventaire dans un système comptable automatisé approuvé par le CST;
- lorsqu'un sous-compte COMSEC a en sa possession un MCC qui ne figure dans aucun inventaire de compte COMSEC.

NOTA : Certaines des circonstances qui précèdent peuvent également exiger du gardien de sous-compte COMSEC qu'il signale un incident COMSEC. Lorsque rien ne permet d'établir avec certitude si un incident a eu lieu ou non, prière de communiquer avec le CCIC pour obtenir des conseils.

7.4.3.2 Préparation

Sauf dans les situations détaillées à la section 11.3.2.5 et dans l'ITSD-08, un sous-compte COMSEC doit obtenir l'autorisation du CCIC avant de soumettre un *rapport de possession*. Les directives suivantes s'appliquent à la préparation et à la distribution *des rapports de possession* :

- il faut inclure une brève description du motif de la possession dans la colonne « Remarques » ou sous la ligne « NOTHING FOLLOWS – RIEN NE SUIT »;
- lorsque le rapport comprend du matériel COMSEC comptabilisé au NCOR, il faut envoyer un exemplaire au CCIC dans les cinq jours ouvrables suivant la création du rapport; *les rapports de possession* dans lesquels figure uniquement du matériel CC 4 ou CC 7 doivent être conservés localement.

7.4.3.3 Distribution

La distribution du *Rapport de possession* doit se faire comme suit :

- envoyer l'exemplaire originale signé au CCIC;
- conserver un exemplaire dans les dossiers;
- lorsqu'il s'agit de MCC reçu sans *rapport de matériel COMSEC* et que la source du matériel est connue, envoyer un exemplaire à la source.

7.4.4 Dispense de la comptabilité

Le *Rapport de dispense de la comptabilité* (GC-223) sert à consigner le retrait d'un MCC de l'inventaire d'un sous-compte COMSEC.

Un gardien de sous-compte COMSEC peut demander d'être dispensé de la comptabilité d'un MCC qui a été irrémédiablement perdu.

7.4.5 Rapport de destruction

En temps normal, une entreprise du secteur privé pourra détruire une clé COMSEC comptable seulement lorsqu'une lettre sur l'état du matériel produite par le CCIC l'y autorise (voir la section 12.2). Le *Rapport de destruction* (GC-223) sert à consigner la destruction physique ou la mise à zéro électronique du MCC par des moyens autorisés ou de manière accidentelle; il permet de signaler les articles qui ont été retirés de la comptabilité (voir la section 12).

7.4.5.1 Préparation et distribution

Les directives suivantes s'appliquent à la préparation et à la distribution du *Rapport de destruction :*

- les clés devant être détruites doivent être énumérées en ordre alphanumérique;
- il faut indiquer le motif de la destruction (p. ex. clé mise à zéro, remplacée);
- il faut en envoyer, au CCIC, un exemplaire signé du *Rapport de destruction*, lorsque celui-ci inclut des clés CC 1, CC 2, CC 4, CC 6 ou CC 7;
- il faut conserver, dans les dossiers, un exemplaire signé du *Rapport de destruction*.

7.4.6 Rapport de destruction consolidé

Le *Rapport de destruction consolidé* (GC-223) ne doit être préparé que lorsque d'autres documents de destruction le justifient (p. ex. fiches HI/DR). Avant de produire le rapport qui répertorie l'édition complète de clés, le personnel de garde doit confirmer la destruction de tous les segments de clé de l'édition.

En pareils cas, la personne ayant effectué la destruction doit transmettre au CCIC les documents de destruction appropriés, dûment signés par elle et par un témoin.

7.4.6.1 Préparation et distribution

Les directives suivantes s'appliquent à la préparation et à la distribution du *Rapport de destruction consolidé :*

- il faut examiner les documents de destruction locale (p. ex. fiches HI/DR) pour s'assurer qu'ils sont exacts et qu'ils comportent les autorisations et les signatures appropriées;
- le rapport doit énumérer les clés qui ont été détruites (et signalées comme ayant été détruites dans les registres comptables locaux) durant le mois;
- le rapport doit porter la mention « *Rapport de destruction consolidé* »;
- il faut soumettre le rapport au CCIC au plus tard le 16^{e} jour du mois suivant la destruction des clés, lorsque le rapport contient des clés CC 1, CC 2, CC 4, CC 6 ou CC 7;
- un exemplaire signé de tous les *rapports de destruction consolidés* doit être conservé en dossier.

7.5 Rapport de conversion de clés de diversification

L'Installation centrale canadienne (ICC) produit chaque mois un *rapport de conversion de clés de diversification* (SKCR pour *Seed Key Conversion Report*) pour l'équipement compatible avec le protocole d'interopérabilité des communications sécurisées (SCIP pour *Secure Communication Interoperability Protocol*). Ce rapport contient l'identificateur de matériel de chiffrement (KMID pour *Key Material Identifier*) des clés de diversification qui ont été converties en clés opérationnelles durant le mois.

Lorsqu'un titulaire de prêts se sert d'un équipement SCIP autorisé pour établir un appel sécurisé avec le sous-système de remise à la clé du Réseau téléphonique public commuté – Réseau numérique à intégration de services (RTPC-RNIS) du Secure Data Networking System (SDNS) – ou SPIRS (pour *SDNS Public Switched Telephone Network–Integrated Services Digital Network Rekey Subsystem*) – une clé opérationnelle est envoyée à l'équipement SCIP du titulaire de prêts.

Une fois l'opération terminée, le titulaire de prêts peut désormais se servir de son équipement pour établir des appels sécurisés avec d'autres utilisateurs SCIP. Un exemplaire du SKCR est envoyé par le CCIC au gardien du sous-compte COMSEC chaque mois ou à sa demande. Le gardien du sous-compte COMSEC doit l'utiliser pour confirmer auprès du CCIC qu'un *rapport de destruction* a été créé pour tous les KMID figurant dans le SKCR.

7.6 Rapport de remise à la clé opérationnelle

L'ICC produit chaque mois un *Rapport de remise à la clé opérationnelle* (ORR pour *Operational Rekey Report*) qui énumère les KMID de l'équipement SCIP servant à établir un appel sécurisé avec le SPIRS. Lorsqu'un utilisateur établit un appel sécurisé avec le SPIRS, une nouvelle clé opérationnelle est téléchargée dans l'équipement SCIP de l'utilisateur, de même qu'une liste des clés compromises (CKL pour *Compromised Key List*). Le CCIC envoie un exemplaire de l'ORR au gardien de sous-compte COMSEC tous les mois ou sur demande. Ce rapport doit être utilisé pour vérifier si les utilisateurs appellent le SPIRS tous les trois mois pour effectuer une remise à la clé et s'ils ont la CKL la plus récente. Le CCIC doit se servir de l'ORR pour vérifier si un *Rapport de destruction* a été rempli pour tous les KMID figurant dans l'ORR.

7.7 Rapport d'inventaire

Les gardiens de sous-compte COMSEC sont responsables de la prise des inventaires. Durant le processus d'inventaire, le MCC détenu par le sous-compte COMSEC fait l'objet d'un contrôle visuel, et les articles en stock sont comparés aux dossiers comptables. Le processus d'inventaire est très important, car c'est parfois le seul moyen de découvrir la perte d'un MCC. Pour de l'information détaillée sur les *rapports d'inventaire*, prière de consulter la section 13.

7.8 Avis de recherche

7.8.1 Accusé de réception

Lorsque le CCIC n'a pas reçu d'*accusé de réception* signé dans les 20 jours ouvrables suivant la date d'envoi, le CCIC enverra un *Avis de recherche* au sous-compte COMSEC fautif.

7.8.2 Rapport d'inventaire

Il est impossible d'effectuer le rapprochement de l'inventaire du sous-compte COMSEC lorsque des *rapports d'inventaire* sont manquants. En l'occurrence, le CCIC lance une demande de recherche pour les *rapports de matériel COMSEC* manquants.

7.9 Omission de répondre aux avis de recherche

S'il néglige de répondre aux *avis de recherche* qui lui ont été envoyés, le sous-compte COMSEC fautif risque de faire immédiatement l'objet d'une vérification qu'effectuera un représentant ou un vérificateur désigné par le CCIC.

Si la demande de recherche initiale et l'aide du CCIC ne suffisent pas à résoudre le problème, un *avis de recherche* secondaire doit être envoyé à l'ASE afin qu'il prenne les mesures appropriées (notamment une enquête visant à établir si un incident COMSEC a eu lieu).

8 Accès au matériel COMSEC comptable

8.1 Conditions préalables à l'accès au matériel COMSEC comptable

8.1.1 Accès par les employés d'une entreprise du secteur privé

L'accès au MCC peut être accordé aux citoyens canadiens (pouvant posséder une double nationalité) qui répondent aux critères suivants :

- détenir une habilitation de sécurité valide correspondant à la classification de sécurité du matériel et de l'information auxquels ils ont accès;

  NOTA : Voir la section 3.1 pour obtenir plus de détails sur les exigences concernant l'habilitation de sécurité des gardiens de sous-compte COMSEC et des gardiens suppléants.

- pouvoir démontrer un besoin de connaître;
- avoir assisté à une séance d'initiation COMSEC;
- avoir signé une attestation d'initiation COMSEC;
- connaître suffisamment les procédures de contrôle du matériel COMSEC applicables;
- avoir été désigné comme gardien de sous-compte COMSEC, gardien de compte COMSEC IP, gardien suppléant, titulaire de prêts ou utilisateur autorisé, être appelé à utiliser du MCC dans l'exercice de ses fonctions et à être responsable dudit MCC.

8.1.2 Accès par des ressortissants étrangers

Les Services à la clientèle en matière de COMSEC peuvent approuver, au cas par cas, l'accès au MCC par des ressortissants étrangers (c.-à-d. des citoyens non canadiens). À cet égard, l'ACM doit soumettre une demande écrite aux Services à la clientèle en matière de COMSEC.

8.1.3 Exigences relatives à la participation aux demandes de propositions du gouvernement du Canada

Une entreprise du secteur privé ne peut être empêchée de participer à une demande de propositions (DP) du GC exigeant l'accès à du MCC pour le seul motif qu'elle n'a pas établi de sous-compte COMSEC avant de présenter son offre. Toute entreprise qui désire présenter une DP et qui ne détient pas de sous-compte COMSEC doit communiquer avec les Services à la clientèle en matière de COMSEC pour demander une évaluation de la pertinence d'obtenir un tel sous-compte dans l'éventualité où elle se verrait adjuger un contrat. L'entreprise doit être en mesure de satisfaire aux conditions préalables à l'établissement d'un sous-compte COMSEC, tel qu'il est détaillé dans la présente directive, avant de se voir remettre du MCC.

NOTA 1 : Le personnel du PSI doit également évaluer la pertinence des inspections liées à l'ASI, aux TI, à la production, à l'ADR et à la PCIE.

NOTA 2 : Les exigences du PMC (voir la section 1.11.2) doivent être respectées.

8.2 Séance d'initiation COMSEC et attestation d'initiation COMSEC

8.2.1 Exigences

Le CCIC doit tenir une séance d'initiation COMSEC initiale à l'intention du gardien de sous-compte COMSEC; ce dernier doit ensuite s'assurer que toutes les personnes devant avoir accès au MCC suivent cette séance et signent une *attestation d'initiation COMSEC*.

NOTA : Toute personne nommée de nouveau au même sous-compte COMSEC ou à un sous-compte COMSEC différent en tant que gardien de sous-compte COMSEC, gardien suppléant ou titulaire de prêts doit assister à une nouvelle séance d'initiation COMSEC et signer une nouvelle *attestation d'initiation COMSEC*.

Une séance d'initiation COMSEC est requise pour toute personne (y compris les membres du personnel du sous-compte COMSEC, les titulaires de prêts, les personnes participant à des cours et à des forums COMSEC au CST et sur la scène internationale, et les personnes qui ont besoin d'un accès aux fins d'utilisation ou de maintenance durant l'installation, le dépannage, la réparation ou la mise à la clé de l'équipement) qui doit accéder aux éléments suivants :

- du MCC;
- de l'information cryptographique qui contient, décrit ou met en œuvre une logique cryptographique classifiée;
- de l'information cryptographique comprenant, entre autres, les manuels de maintenance intégrale et les logiciels cryptographiques informatiques (doit constituer un besoin permanent);
- un MCC IP ou un CCI classifié et ses composants, et ce, à n'importe quel stade de sa production ou de son développement;
- une clé ou une logique cryptographique en cours de production ou de développement.

8.2.2 Conservation des attestations d'initiation COMSEC

Une *attestation d'initiation COMSEC* pour les personnes ayant accès au MCC d'un sous-compte COMSEC doit être conservée dans les dossiers pendant une période minimale de deux ans après que l'autorisation d'accès au MCC a pris fin.

8.2.3 Rappel des consignes COMSEC et mises à jour

Les rappels de consignes COMSEC ne sont pas nécessaires lorsque l'accès au MCC n'est plus requis. Une mise à jour de la séance d'initiation COMSEC est requise tous les cinq ans dans le cas des gardiens de sous-compte COMSEC, des gardiens suppléants, des titulaires de prêts et des utilisateurs autorisés.

8.3 Intégrité par deux personnes

La TPI est une mesure de sécurité conçue pour empêcher qu'une personne accède seule à un MCC particulier (p. ex. une clé TRÈS SECRET). Chaque personne ayant un accès TPI doit être en mesure de reconnaître, s'il y a lieu, les manquements aux exigences procédurales pendant l'exécution d'une tâche. L'entreposage et la manutention régis par la TPI nécessitent l'utilisation de dispositifs de sécurité protégés par deux verrous approuvés (voir le *Guide d'équipement de sécurité* [G1-001]) de la Gendarmerie royale du Canada [GRC]), deux numéros d'identification personnels (NIP) ou deux mots de passe approuvés, sans qu'une seule personne n'ait accès aux deux combinaisons, clés, NIP ou mots de passe.

NOTA : Pour consulter le guide G1-001, prière de communiquer avec les Services à la clientèle en matière de COMSEC.

8.4 Zone jamais seul

Certains secteurs d'une installation COMSEC peuvent être désignés comme « zones jamais seul » (NLZ). Dans une NLZ, un minimum de deux personnes autorisées doivent être en contact visuel constant l'une de l'autre. Lorsque l'une des deux personnes est appelée à quitter les lieux, l'autre doit quitter en même temps pour éviter de rester seule dans la zone. Dans ce cas, les deux personnes en question ne peuvent quitter sans avoir sécurisé la zone.

L'ASE établira une NLZ pour les sous-comptes COMSEC qui répondent à l'une des conditions suivantes :

- reçoivent, entreposent, manutentionnent, utilisent et détruisent des clés TRÈS SECRET;
- produisent des clés physiques;
- conçoivent, développent, fabriquent ou maintiennent de l'équipement cryptographique.

8.5 Contrôle d'accès – Visites COMSEC

Il incombe à l'ASE de veiller à ce que toutes les visites de l'entreprise au cours desquelles les personnes ont accès au MCC, à de l'information COMSEC protégée et classifiée ou à du matériel lié au MCC soient autorisées par le PSI, lorsqu'un contrat du GC a été conclu.

Une entreprise du secteur privé qui doit accéder au MCC, à de l'information COMSEC protégée et classifiée ou à du matériel lié au MCC en dehors de ses locaux doit présenter une demande de permis de visite par l'entremise du PSI. Le personnel du PSI présentera ensuite une demande d'autorisation d'accès COMSEC aux Services à la clientèle en matière de COMSEC, qui informeront le gestionnaire du CCIC de la demande de visite et de son autorisation ou de son refus.

Les exigences suivantes relatives aux visites au cours desquelles des personnes ont accès au MCC, à de l'information COMSEC protégée et classifiée ou à du matériel lié au MCC doivent être autorisées par les Services à la clientèle en matière de COMSEC :

- un ministère du GC dans une entreprise du secteur privé canadien;

- une entreprise du secteur privé canadien dans un ministère du GC;
- une entreprise du secteur privé canadien dans une entreprise du secteur privé canadien ou étranger;
- une entreprise du secteur privé canadien dans un organisme d'un gouvernement étranger.

NOTA 1 : Les entreprises du secteur privé liées par un contrat doivent s'assurer que le personnel du PSI approuve tous les visiteurs, y compris les ministères du GC, qui doivent avoir accès au MCC.

NOTA 2 : En dépit des exigences du MSI énoncées à la section 2.6.2, un représentant du CCIC n'a **pas** besoin d'obtenir l'autorisation de visite COMSEC du PSI; toutefois, le personnel du PSI doit fournir à l'ASE de l'information sur les visiteurs, tel qu'il est détaillé à la section 8.6.

8.6 Demande de visite COMSEC

Pour les contrats du GC, le personnel du PSI présentera aux Services à la clientèle en matière de COMSEC une demande d'autorisation d'accès COMSEC pour toute visite canadienne dans un organisme gouvernemental étranger ou dans une entreprise du secteur privé (y compris les entreprises étrangères) au cours de laquelle les visiteurs doivent accéder au MCC, à de l'information COMSEC classifiée et protégée ou à du matériel lié au MCC. Cette demande doit être soumise au moins 45 jours civils avant ladite visite.

La demande de visite COMSEC doit contenir les éléments suivants :

- le nom de famille du visiteur;
- tous les prénoms du visiteur;
- la date de naissance (JJ/MM/AAAA) du visiteur;
- le lieu de naissance du visiteur;
- la citoyenneté (y compris la double nationalité) du visiteur;
- le niveau d'habilitation de sécurité du visiteur (vérifié par le personnel de sécurité);
- un exemplaire signé de l'Attestation d'initiation COMSEC;
- le numéro du contrat ou du sous-contrat associé à la visite;
- la raison de la visite (accès COMSEC requis);
- le nom, le numéro de téléphone, le numéro de télécopieur et l'adresse électronique de la personne-ressource de la sécurité à destination;
- le nom, le numéro de téléphone, le numéro de télécopieur et l'adresse électronique de la personne-ressource ou du bureau de première responsabilité correspondant au lieu de la visite;
- l'adresse complète de l'entreprise ou de l'organisme hôte de la visite.

Une fois que les Services à la clientèle en matière de COMSEC ont approuvé l'accès COMSEC et que le personnel du PSI a autorisé la visite, le demandeur doit s'assurer, avant ladite visite, que le permis et l'autorisation d'accès COMSEC ont été émis pour le lieu de la visite. Cette procédure doit être effectuée au moins cinq jours ouvrables avant la visite, afin de permettre la résolution de problème éventuels.

NOTA : Pour les visites à l'étranger, il faut inclure le numéro de passeport et la date d'expiration.

9 Sécurité physique

9.1 Installations COMSEC

9.1.1 Exigence

Il faut établir une installation COMSEC aux endroits où du MCC est produit, entreposé, réparé ou utilisé, ou encore où les activités en justifient la présence (p. ex. aire de travail du gardien de sous-compte COMSEC). Une installation COMSEC est fixe ou mobile. L'installation doit assurer une protection maximale contre le vol, la compromission, les dommages et la détérioration du matériel COMSEC, ainsi qu'assurer l'intégrité de l'accès et de la comptabilité.

Les zones où les gardiens de sous-compte COMSEC travaillent, mais qui sont situées à l'extérieur des installations COMSEC établies (p. ex. structures temporaires, véhicules mobiles) et qui ne sont pas considérées comme des installations COMSEC doivent faire l'objet d'une autorisation de la part des Services à la clientèle en matière de COMSEC.

NOTA : Un environnement de bureau renfermant de l'équipement cryptographique destiné aux utilisateurs et des clés à l'état NOIR (chiffrées – voir la section 11.1.2) n'est pas considéré comme une installation COMSEC; toutefois, l'aire de bureaux doit être protégée à tout le moins au niveau de classification le plus élevé de l'équipement mis à la clé.

9.1.2 Planification et établissement d'une installation COMSEC fixe

Au moment de planifier et d'établir une installation COMSEC fixe, l'ASE doit :

- consulter les Services à la clientèle en matière de COMSEC pour répondre aux exigences énoncées à la section 3 de la présente directive;
- veiller à ce qu'une *évaluation des menaces et des risques* (EMR) soit effectuée une fois, avant l'activation initiale (dans la mesure du possible), et périodiquement par la suite, en fonction des menaces, des modifications physiques, de la sensibilité des opérations et des *rapports d'incident COMSEC* de nature grave;
- établir l'installation COMSEC dans une aire offrant un contrôle intégral (*positive control*) des accès basé sur une hiérarchie de zones (voir la section 6.2 de la *Norme opérationnelle sur la sécurité matérielle* du Secrétariat du Conseil du Trésor du Canada [SCT] et le *Guide pour l'établissement des zones de sécurité matérielle* [G1-026] de la GRC); pour de plus amples détails, prière de communiquer avec le PSI ou les Services à la clientèle en matière de COMSEC;
- construire l'installation COMSEC conformément à la *Norme opérationnelle sur la sécurité matérielle* et au guide G1-026;
- élaborer une procédure normale d'exploitation (en conjonction avec le *Plan d'urgence COMSEC*) qui contient des dispositions pour effectuer les opérations de manière sécurisée.

9.1.3 Contrôles d'accès et restrictions

Le gardien de sous-compte COMSEC doit s'acquitter des tâches suivantes :

- établir une liste d'accès des personnes autorisées qui ont des tâches régulières à exécuter dans l'installation COMSEC;

- limiter l'accès sans escorte aux personnes qui sont des citoyens canadiens (et pouvant avoir une double nationalité), dont les tâches requièrent un tel accès et qui satisfont aux exigences en matière d'accès énoncées à la section 8;
- veiller à ce que tous les visiteurs (y compris le personnel d'entretien ménager) soient inscrits dans un registre des visiteurs et à ce que celui-ci soit conservé pendant au moins un an après la date de la dernière entrée. Le registre des visiteurs doit au moins contenir les renseignements suivants :
  - la date, l'heure d'arrivée et l'heure de départ du visiteur,
  - le nom du visiteur en caractères d'imprimerie,
  - la signature du visiteur,
  - la raison de la visite,
  - la signature, de même que le nom en caractères d'imprimerie, de la personne autorisée ayant admis le visiteur;
- veiller à ce que les visiteurs soient continuellement escortés par une personne autorisée dont le nom figure sur la liste d'accès;
- interdire, dans l'installation COMSEC, les dispositifs et l'équipement non autorisés par le CST qui sont conçus pour capter et enregistrer des images intelligibles, les appareils de prise de son et d'enregistrement, les postes radio émetteurs et récepteurs, les microphones, et les téléviseurs;
- apposer une affiche pour indiquer que l'aire est à ACCÈS RESTREINT;
- établir et consigner une procédure de contrôle de sécurité quotidienne afin d'assurer la protection appropriée du MCC et le bon fonctionnement des dispositifs approuvés de protection de la sécurité physique (p. ex. verrous de porte, système d'alarme);
- veiller à ce que les installations sans personnel situées dans des endroits où les risques de compromission sont élevés utilisent un système de détection d'intrusion conforme à la norme ULC-S306-03, des Laboratoires des assureurs du Canada (ULC pour *Underwriters Laboratories of Canada*); des contrôles sur place doivent être effectués au moins une fois toutes les 24 heures pour s'assurer que les portes sont verrouillées et que personne n'a tenté de pénétrer de force dans les locaux.

9.2 Approbation de l'installation COMSEC

Toute installation nouvelle, rénovée ou déplacée servant d'aire de travail du gardien de sous-compte COMSEC doit être approuvée par le CCIC avant qu'une entreprise du secteur privé ne soit autorisée à recevoir du MCC. Le personnel du CCIC, à la suite d'une visite de l'installation, accordera une autorisation si l'installation satisfait aux exigences en matière de protection du MCC, lesquelles sont énoncées dans la présente directive.

NOTA : Cette exigence s'ajoute aux exigences des inspections liées à l'ASI, l'ADR et aux TI, ou aux exigences équivalentes de l'IMPC.

9.3 Entreposage sécurisé

9.3.1 Contenants de sécurité

Le MCC doit être entreposé dans des contenants de sécurité (p. ex. chambre forte, coffre-fort, classeur, etc.) approuvés pour le niveau de classification ou de protection du MCC et conformes aux exigences stipulées dans le guide G1-001 de la GRC.

Les contenants de sécurité servant à entreposer le MCC doivent être situés dans une zone de sécurité appropriée au niveau de classification du MCC. Pour obtenir des directives supplémentaires sur l'utilisation et l'acquisition de contenants de sécurité, prière de communiquer avec la PSI ou les Services à la clientèle en matière de COMSEC.

NOTA 1 : Les porte-documents ne sont pas considérés comme des contenants d'entreposage et ne doivent pas être utilisés comme tels.

NOTA 2 : Pour consulter le guide G1-001 de la GRC, prière de communiquer avec les Services à la clientèle en matière de COMSEC.

9.3.2 Séparation du matériel COMSEC entreposé

Les règles de séparation minimale visant l'entreposage du MCC sont les suivantes :

- les éditions en vigueur, les éditions en réserve et les clés remplacées en attente de destruction doivent être entreposées séparément les unes des autres dans des contenants de sécurité approuvés (voir le guide G1-001 de la GRC);

  NOTA : Pour consulter le guide G1-001 de la GRC, prière de communiquer avec les Services à la clientèle en matière de COMSEC.

- les clés ou les clés de contact cryptographiques (CIK) ne doivent pas être entreposées dans le même contenant de sécurité que l'équipement connexe.

  NOTA : Là où l'espace est limité, une telle séparation peut être réalisée au moyen d'un coffret de sécurité verrouillé, rangé dans un même contenant de sécurité.

9.3.3 Ouverture des contenants de sécurité en cas d'urgence

Lorsque le gardien de sous-compte COMSEC et le gardien suppléant ne sont pas disponibles pour ouvrir un contenant de sécurité lors d'une situation d'urgence, l'ASE (ou toute autre autorité pertinente) peut demander l'ouverture du contenant, dans les conditions suivantes :

- au moins deux personnes doivent être présentes pour accéder à la combinaison et ouvrir le contenant de sécurité;
- les personnes qui ont ouvert d'urgence le contenant de sécurité doivent préparer un rapport écrit (qui décrit le contenu et les circonstances justifiant le besoin d'y accéder) pour la ou les personnes responsables du contenant de sécurité;
- la ou les personnes responsables du contenant de sécurité doivent dresser l'inventaire complet du MCC et changer la ou les combinaisons immédiatement après leur retour.

La personne nécessitant un accès immédiat au contenant de sécurité doit communiquer avec le gardien de sous-compte COMSEC ou le gardien suppléant, advenant une situation d'urgence où il faut accéder à du MCC déjà remis à un titulaire de prêts qui n'est pas disponible.

9.3.4 Incidents liés aux contenants de sécurité laissés sans surveillance

Dans le cas d'un incident de sécurité (p. ex. quelqu'un découvre la chambre forte ou un contenant ouvert et laissé sans surveillance pendant ou après les heures normales de travail), la personne ayant fait la découverte doit avertir le gardien de sous-compte COMSEC ou le gardien suppléant. S'il n'est possible de joindre ni le gardien de sous-compte COMSEC ni le gardien suppléant, il faut communiquer avec l'un des titulaires de clés inscrits à la liste ou avec un responsable qui connaît les combinaisons du contenant. Le gardien de sous-compte COMSEC et le gardien suppléant doivent dresser un inventaire complet du contenu du contenant et sécuriser le contenant (p. ex. en fournissant un nouveau verrou ou en changeant la combinaison sur-le-champ).

Advenant un incident touchant du MCC remis à un titulaire de prêts, la personne ayant découvert l'incident doit communiquer avec le gardien de sous-compte COMSEC ou le gardien suppléant.

9.4 Protection des combinaisons et des clés de serrures

9.4.1 Généralités

Il faut signaler sans délai au CCIC toute indication de trafiquage ou tout soupçon de compromission d'une serrure ou de sa combinaison (ou clé).

9.4.2 Changement des combinaisons

Le gardien de sous-compte COMSEC doit veiller à ce qu'une personne autorisée par l'ASE modifie les combinaisons des serrures utilisées pour l'entreposage sécurisé du MCC lorsque survient l'une des occurrences suivantes :

- la serrure est mise en service pour la première fois par le gardien de sous-compte COMSEC (la combinaison réglée en usine par le fabricant ne doit pas être utilisée);
- une personne qui connaît la combinaison n'est plus autorisée à accéder à l'installation d'entreposage ni au contenant de sécurité;
- une personne non autorisée a eu accès à l'enregistrement écrit de la combinaison;
- la combinaison a été présumément ou effectivement compromise;
- la serrure a été réparée, entretenue ou inspectée par une personne qui n'est pas autorisée à accéder à l'installation d'entreposage ou au contenant de sécurité;
- la combinaison n'a pas été changée depuis 12 mois;
- la serrure a été mise hors service, de façon temporaire ou permanente.

9.4.3 Sélection des combinaisons

Chaque serrure doit avoir une combinaison formée de numéros sélectionnés au hasard, conformément aux spécifications du fabricant. Une combinaison ne doit pas être identique à celle d'une autre serrure au sein de l'installation. Les recommandations additionnelles suivantes s'appliquent aux numéros des combinaisons :

- ils ne doivent comprendre ni dates de naissance, ni numéros de salle, ni adresses municipales, etc.;
- ils doivent être séparés de la manière suivante :
  - dans des classeurs dotés de serrures intégrées – les numéros des cadrans numériques sont divisés en deux groupes : petits numéros (0 à 49) et grands numéro (50 à 99),
  - dans des cadenas à combinaisons – les numéros des cadrans numériques sont également divisés en deux groupes : petits numéros (0 à 24) et grands numéros (25 à 49);
- chaque numéro doit être séparé du suivant par au moins 10 numéros;
- dans le cas des classeurs dotés de serrures intégrées, les combinaisons ne doivent pas comprendre de numéros entre 90 et 10, et le troisième numéro ne doit pas se situer entre 90 et 20.

9.4.4 Classification des combinaisons

Les combinaisons de serrure ou de chambre forte doivent être classifiées au niveau correspondant au niveau de sensibilité le plus élevé de l'information ou du matériel protégés.

9.4.5 Changement des serrures à clé

Le gardien de sous-compte COMSEC doit veiller à ce qu'une serrure à clé servant à sécuriser le MCC soit remplacée et non réutilisée pour sécuriser un autre MCC, lorsque survient l'une des occurrences suivantes :

- une personne n'est plus autorisée à accéder au contenant de sécurité;
- une personne non autorisée a eu accès à une clé de la serrure;
- la clé ou la serrure été ont été effectivement ou présumément compromises;
- la serrure a été réparée, entretenue ou inspectée par une personne qui n'est pas autorisée à accéder au contenant de sécurité;
- la serrure n'a pas été changée depuis 12 mois.

9.4.6 Protection des combinaisons et des clés de rechange

Lorsque la personne responsable du contenant de sécurité a changé la serrure à combinaison ou la serrure à clé, le gardien de sous-compte COMSEC doit s'assurer que cette personne a fait ce qui suit :

1. ranger la combinaison (ou les clés de rechange) dans une enveloppe opaque scellée, de façon à ce que l'éventuel trafiquage de cette dernière soit apparent;
2. inscrire, sur l'enveloppe, le niveau de classification ou de protection le plus élevé du MCC protégé par la combinaison (ou les clés), de même que le nom et le numéro de téléphone des personnes autorisées à accéder à la combinaison (ou aux clés);
3. remettre l'enveloppe au gardien de sous-compte COMSEC pour qu'elle soit rangée dans un contenant de sécurité dont le niveau de classification ou de protection est égal ou supérieur à celui du matériel protégé par la combinaison (ou les clés).

9.4.7 Registre des combinaisons et des clés

Le gardien de sous-compte COMSEC doit tenir un registre des noms et numéros de téléphone des personnes qui connaissent les combinaisons (ou qui détiennent une clé) des contenants dans lesquels du MCC est entreposé. En temps normal, les contenants sont placés sous le contrôle direct du gardien de sous-compte COMSEC et du gardien suppléant.

9.4.8 Accès aux clés et aux combinaisons et connaissance de ces dernières

Le gardien de sous-compte COMSEC doit veiller à ce que seules les personnes autorisées et détenant une habilitation de sécurité appropriée aient accès aux combinaisons (ou aux clés) qui protègent le MCC dont ils ont la garde, et connaissent ces combinaisons. Les membres du personnel connaissant les combinaisons ne doivent pas consigner celles-ci par écrit ni garder cette information sur eux; ils ne doivent pas non plus les conserver sous forme électronique. Les clés ne doivent pas être conservées dans un tableau des clés accessible à des personnes autres que le gardien de sous-compte COMSEC ou le gardien suppléant.

9.4.9 Combinaisons pour les contenants contrôlés par deux personnes ou situés dans des zones jamais seul

Le gardien de sous-compte COMSEC doit s'assurer qu'aucun des intervenants concernés ne soit autorisé à voir, à connaître ou à modifier les deux combinaisons d'un contenant de sécurité utilisé pour entreposer du matériel COMSEC nécessitant un contrôle TPI ou se trouvant dans une NLZ.

NOTA : Les combinaisons de serrure doivent être classifiées et protégées au niveau de sécurité le plus élevé du matériel qu'elles protègent.

9.5 Entreposage des clés cryptographiques

9.5.1 Exigences relatives à l'entreposage des clés physiques

Les clés qui ne sont pas sous la surveillance directe et continue d'une personne habilitée et autorisée (ou de plusieurs personnes, le cas échéant) doivent être entreposées dans un contenant de sécurité approuvé et verrouillé (voir le guide G1-001 de la GRC) se trouvant dans une aire protégée par des gardiens de sécurité ou par un système de détection d'intrusion (c.-à-d. zone de sécurité, zone de haute sécurité). Prière de consulter le Tableau 4 pour les exigences particulières liées à l'entreposage des clés physiques.

Tableau 4 – Entreposage des clés physiques

Clés	Exigences en matière d'entreposage
Clés TRÈS SECRET ou autres clés nécessitant un contrôle TPI	Les clés TRÈS SECRET doivent être entreposées selon le principe TPI dans des contenants respectant les normes énoncées dans le guide G1-001 de la GRC. Une clé TRÈS SECRET détenue dans une aire de travail pour y être utilisée à divers moments de la journée peut être protégée par une seule serrure dans une NLZ. Seul le superviseur en fonction peut connaître la combinaison ou avoir accès à la clé de la serrure.

Clés	Exigences en matière d'entreposage
	Voici les façons dont on peut disposer d'une clé TRÈS SECRET dans les environnements tactiques : • entreposer dans un coffre-fort de terrain standard et approuvé; • entreposer dans un contenant semblable protégé par une serrure à combinaison conforme aux normes du guide G1-001 de la GRC; • conserver sous garde personnelle (à défaut d'installations adéquates d'entreposage).
Clés SECRET, CONFIDENTIEL et PROTÉGÉ C	Les clés SECRET, CONFIDENTIEL et PROTÉGÉ C doivent être entreposées de l'une des deux façons suivantes : • conformément à toute procédure approuvée pour les clés TRÈS SECRET; • dans un contenant approuvé pour du matériel SECRET, CONFIDENTIEL ou PROTÉGÉ C, selon le cas, doté d'une serrure à combinaison approuvée.
Clés PROTÉGÉ A et PROTÉGÉ B	Les clés PROTÉGÉ A et PROTÉGÉ B doivent être entreposées conformément à une procédure approuvée pour une clé classifiée.
Clés NON CLASSIFIÉ	Les clés NON CLASSIFIÉ doivent être entreposées selon le moyen le plus sécurisé dont dispose l'utilisateur autorisé, à la condition que cet utilisateur assure une protection raisonnable contre le vol, le sabotage, le trafiquage ou l'utilisation par des personnes non autorisées.
Clés étrangères	Les clés étrangères doivent être entreposées conformément aux consignes qui s'appliquent au matériel COMSEC canadien de sensibilité équivalente. Une clé étrangère portant la mention *UNCLASSIFIED, RESTRICTED* ou *UNCLASSIFIED/For Official Use Only* (U//FOUO) et marquée CRYPTO doit être entreposée comme du matériel COMSEC PROTÉGÉ A (ou de niveau supérieur).
Entreposage ouvert	Entreposage d'information classifiée de sécurité nationale en dehors des contenants approuvés, ce qui comprend l'information classifiée enregistrée sur un support de système d'information et en dehors d'un contenant d'entreposage approuvé, que ce support soit en cours d'utilisation ou non (c.-à-d. support laissé sans surveillance). L'entreposage « ouvert » d'équipement et de matériel cryptographiques classifiés doit être réalisé dans une installation COMSEC, une chambre forte ou une salle sécurisée approuvée, lorsqu'aucun membre du personnel autorisé n'est présent. Sauf pour l'entreposage d'une clé TRÈS SECRET, les contrôles TPI et NLZ ne sont PAS requis.

9.5.2 Clés gardées en réserve

La quantité de clés à garder en réserve dépend de la fréquence de remplacement des clés. Le Tableau 5 – *Clés gardées en réserve* donne un aperçu de la quantité que l'on devrait normalement garder en réserve. Pour des quantités de clés supérieures, prière de communiquer avec le CCIC.

Tableau 5 – Clés gardées en réserve

Fréquence de remplacement	En réserve
Clé remplacée quotidiennement, 10 fois par mois, deux fois par mois et mensuellement.	Éditions en vigueur durant le mois courant, plus une réserve de trois mois.
Clé remplacée tous les deux mois ou trimestriellement.	Édition en vigueur, plus une réserve de deux éditions.
Clé remplacée tous les deux ans, annuellement et sporadiquement.	Édition en vigueur, plus une réserve d'une édition.
Clé de diversification SDNS (facteur de conservation de cinq ans).	Une clé de diversification peut être gardée en réserve.

9.5.3 Entreposage des clés électroniques

Les clés électroniques doivent être entreposées conformément à la doctrine portant sur l'équipement.

9.6 Entreposage de l'équipement cryptographique

9.6.1 Généralités

Lorsqu'il n'est pas sous la surveillance directe et continue d'un membre du personnel habilité et autorisé, l'équipement cryptographique doit être entreposé conformément à son niveau de classification ou de protection et à ses mentions de sécurité (p. ex. CRYPTO, CCI). Cet équipement peut exiger des procédures ou des installations d'entreposage particulières. Pour obtenir plus de détails sur l'entreposage de l'équipement cryptographique, prière de consulter la doctrine portant sur l'équipement en question ou de communiquer avec le CCIC.

NOTA : Il faut entreposer l'équipement cryptographique NON CLASSIFIÉ et les CCI non mis à la clé de façon à assurer une protection raisonnable contre la compromission, le vol, le trafiquage et les dommages.

9.6.2 Préparation en vue de l'entreposage

L'équipement cryptographique comptable ne doit jamais être entreposé lorsqu'il est mis à la clé, sauf dans les cas suivants :

- lorsque des exigences opérationnelles le justifient et qu'il n'existe aucune autre solution pratique;

  NOTA : L'autorisation du CCIC est requise.

- lorsque l'équipement ne peut être mis à zéro en raison d'une défaillance ou d'un dommage.

Lorsqu'on doit entreposer un équipement cryptographique mis à la clé, celui-ci doit être protégé conformément au niveau de classification le plus élevé des clés qui y sont chargées.

NOTA 1 : Les CCI qui utilisent une CIK sont considérés comme déverrouillés lorsque la CIK y est insérée, et verrouillés lorsque la CIK est retirée et inaccessible aux personnes non autorisées.

NOTA 2 : Les CCI dont le mode sécurisé est déverrouillé seulement au moyen d'un NIP sont considérés comme étant déverrouillés dès que le NIP a été entré.

NOTA 3 : Les CCI qui utilisent une combinaison CIK et mot de passe ou NIP sont considérés comme déverrouillés lorsque la CIK est insérée et le mot de passe ou NIP approprié a permis l'authentification.

9.6.3 Équipement cryptographique de secours ou de réserve

L'équipement cryptographique de secours ou de réserve qui se trouve dans une aire de travail sécurisée est considéré comme étant installé à des fins opérationnelles. Les exigences d'entreposage énoncées dans les sections précédentes ne s'appliquent pas à un tel équipement.

9.7 Entreposage des publications COMSEC comptables

Les publications COMSEC doivent être entreposées conformément à leur classification de sécurité de même qu'aux mises en garde ou autres mentions de sécurité qui y sont apposées.

10 Distribution et réception du matériel COMSEC comptable

10.1 Généralités

Le CCIC est l'autorité en matière de déplacement du MCC à l'extérieur d'un sous-compte COMSEC.

10.2 Transfert à destination ou en provenance d'un intérêt étranger

Le transfert de MCC à destination ou en provenance d'un intérêt étranger (comptes COMSEC établis du gouvernement ou du secteur privé) doit être effectué seulement entre les agences nationales de distribution (AND) des gouvernements concernés. Le CCIC (en collaboration avec les Services à la clientèle en matière de COMSEC) doit autoriser le transfert par l'entremise des AND responsables.

10.3 Transmission de clés au moyen des systèmes de télécommunications

À moins d'utiliser des systèmes cryptographiques spécialement conçus et autorisés pour la remise à la clé à distance, les variables de clé opérationnelle doivent être transmises au moyen de méthodes de télécommunications uniquement en situation d'urgence et selon les conditions suivantes :

- le CCIC doit approuver au préalable la transmission des variables de clé opérationnelle;
- un système cryptographique assurant un chiffrement intégral doit être employé (c.-à-d. sans afficher les paramètres de chiffrement en clair dans la voie de communication);
- le système de transmission doit être mis à la clé avec des paramètres classifiés ou protégés à un niveau égal ou supérieur à celui de la clé transmise.

10.4 Distribution de matériel COMSEC comptable à l'extérieur d'un sous-compte

Le gardien de sous-compte COMSEC, en collaboration avec le CCIC, est responsable de veiller à ce que les envois individuels de MCC respectent le minimum requis pour répondre aux exigences contractuelles.

Lorsqu'il prépare le MCC aux fins de distribution, le gardien de sous-compte COMSEC doit procéder à ce qui suit :

- s'assurer que le destinataire dispose d'installations qui satisfont aux exigences d'entreposage de MCC (voir la section 9.3) et effectuer la vérification des pages, la vérification de l'équipement ainsi que l'inspection du conditionnement protecteur dans les 48 heures précédant l'emballage;
- mettre à zéro ou retirer les CIK de tous les CCI avant leur transport (lorsque les circonstances le justifient, les dispositifs mis à la clé peuvent être transportés par les messagers autorisés de l'entreprise du secteur privé);
- emballer les clés opérationnelles et de diversification séparément de l'équipement cryptographique connexe (y compris les CCI) et les expédier dans des véhicules distincts et à des dates différentes, à moins que se produise l'une des occurrences suivantes :
  - l'application ou la conception de l'équipement ne permet pas de séparer physiquement les clés correspondantes,
  - il s'agit de clés de maintenance NON CLASSIFIÉ (qui peuvent être expédiées dans le même contenant que l'équipement cryptographique connexe),
  - il n'existe aucun autre moyen d'effectuer la livraison pour répondre à un besoin opérationnel immédiat;

    NOTA 1 : Lorsque l'équipement cryptographique doit être expédié en état de mise à la clé ou avec la clé connexe, le colis doit être expédié conformément au niveau de classification de la clé ou de l'équipement cryptographique, selon le niveau le plus élevé.

    NOTA 2 : Une entreprise du secteur privé ne doit pas expédier l'équipement cryptographique en état de mise à la clé sans l'autorisation du CCIC.
- envoyer, à différentes dates, la liste des dates d'entrée en vigueur des éditions de clé séparément des clés elles-mêmes;
- emballer chaque clé de chiffrement du trafic (TEK pour *Traffic Encryption Key*) séparément de la KEK connexe;
- emballer séparément les composants qui constituent un système cryptographique (c.-à-d. l'équipement cryptographique de base, les accessoires, la documentation connexe et les variables de clé) et les expédier dans des envois différents;
- appliquer les contrôles TPI aux clés TRÈS SECRET durant leur transit, à moins qu'elles ne soient dans un conditionnement protecteur du fabricant et sous enveloppe double (dans ce cas, un seul messager suffit);
- veiller à ce que les clés électroniques soient transmises conformément à la doctrine du système ou de l'équipement applicable;
- préparer un *rapport de matériel COMSEC* conformément à la section 7.

10.5 Distribution de clés électroniques sur support de stockage amovible magnétique ou optique

En plus des critères énoncés à la section 10.4, il faut savoir qu'un support de stockage amovible (SSA) magnétique ou optique sur lequel une clé électronique est distribuée (c.-à-d. transférée ou remise) doit être contrôlé comme un article COMSEC distinct dans le SNCMC au titre de CC 4. Le gardien de sous-compte COMSEC doit apposer au SSA une étiquette semblable à celle qui est illustrée à la Figure 2 – *Exemple*

d'étiquette de support de stockage amovible magnétique ou optique. Le numéro comptable est le « premier numéro disponible » figurant dans le registre où le gardien de sous-compte COMSEC consigne les numéros de série séquentiels des SSA. Le gardien de sous-compte COMSEC doit préparer et traiter un *rapport de possession* (GC-223) conformément aux prescriptions de la section 7 de façon à inscrire le nouveau MCC dans le SNCMC avant de distribuer le SSA (contenant la clé électronique).

Deux *rapports de transfert* (GC-223) sont requis : l'un pour la comptabilité du SSA servant au transport, l'autre pour la comptabilité du transfert de la clé électronique transportée. Les deux rapports doivent être signés et retournés au compte COMSEC expéditeur.

Si des clés à l'état ROUGE (non chiffrées – voir la section 11.1.2) sont transportées sur un SSA magnétique ou optique, l'étiquette apposée au SSA doit également comporter la mention CRYPTO et indiquer le niveau de classification le plus élevé des clés transportées (au minimum SECRET).

Classification :	SECRET (CRYPTO, le cas échéant)
Code de comptabilité :	CC 4
Titre abrégé :	CAKAE 4005 (+ numéro de compte COMSEC)
Numéro comptable :	(premier numéro disponible de la séquence)

Figure 2 – Exemple d'étiquette de support de stockage amovible magnétique ou optique

10.6 Suivi des envois de matériel COMSEC comptable

Le gardien de sous-compte COMSEC doit s'acquitter des tâches suivantes :

- informer le destinataire des détails de l'envoi et de l'heure approximative de livraison dans les 24 heures suivant l'envoi;
- s'assurer que les numéros de téléphone des sous-comptes COMSEC expéditeur et destinataire figurent sur la lettre de transport lorsque le MCC est expédié par l'intermédiaire d'un transporteur commercial ou des messageries prioritaires de Postes Canada;
- conserver un enregistrement local de l'envoi;
- faire le suivi de l'envoi afin de s'assurer que le MCC a été livré au destinataire autorisé dans les délais prescrits et appliquer les conditions suivantes :
  - si aucun envoi n'a été reçu dans les 48 heures suivant la date de livraison initiale prévue, lancer une mesure de suivi auprès du transporteur pour déterminer le dernier emplacement connu de l'envoi,
  - si l'envoi ne peut être localisé et s'il n'est pas récupéré dans les 24 heures suivant le lancement de la mesure de suivi, supposer qu'il a été perdu en cours de route et signaler immédiatement la perte comme un **incident COMSEC**, tel qu'il est décrit à la section 16.

10.7 Emballage du matériel COMSEC comptable

10.7.1 Aperçu

L'emballage utilisé pour la distribution du MCC physique dépendra de la taille, du poids et de la forme de ce dernier, de même que du moyen de transport utilisé. Tout le MCC doit être expédié dans un emballage double, ou encore déposé dans deux contenants opaques, et soigneusement cacheté (y compris les joints) avant son transport.

NOTA : Les enveloppes à fenêtre ou toute autre forme d'emballage transparent, tel l'enrobage plastique, ne sont pas considérées comme conformes aux normes d'emballage.

10.7.2 Emballage intérieur

L'emballage intérieur doit présenter les caractéristiques suivantes :

- être conçu de façon à détecter tout signe de trafiquage;
- protéger le MCC contre les dommages;
- afficher les renseignements suivants :
  - l'adresse complète des comptes COMSEC expéditeur et destinataire,
  - le niveau de classification ou de protection le plus élevé du contenu,
  - la mise en garde CRYPTO, si l'un des articles contenus dans l'envoi porte cette mention,
  - l'inscription « NE PEUT ÊTRE OUVERT QUE PAR LE PERSONNEL DE GARDE COMSEC ».

L'enveloppe scellée contenant les exemplaires du *rapport de matériel COMSEC* peut être placée dans le colis ou collée sur la surface extérieure de l'emballage intérieur du colis. Lorsque l'envoi comporte plus d'un colis, l'enveloppe peut être placée dans le premier colis de la série ou collée sur ce dernier.

NOTA : Le conditionnement protecteur (p. ex. les distributeurs de clés) n'est pas considéré comme un emballage intérieur lors de la préparation des articles aux fins d'expédition (voir la section 11.1.4).

10.7.3 Emballage extérieur

L'emballage extérieur doit présenter les caractéristiques suivantes :

- être suffisamment sécurisé pour empêcher tout dommage du contenu ou tout déballage accidentel;
- ne porter aucune indication que le colis contient du MCC classifié ou protégé;
- afficher les renseignements suivants :
  - l'adresse complète des comptes COMSEC expéditeur et destinataire,
  - le numéro d'envoi ou le numéro du messager autorisé,
  - le numéro du colis suivi d'une barre oblique (/) et du nombre total de colis faisant partie de l'envoi (p. ex. 1/3, 2/3, 3/3), le cas échéant;
- comporter toute la documentation douanière requise, apposée clairement à l'emballage.

10.7.4 Types d'emballage

10.7.4.1 Enveloppes

Des enveloppes doubles officielles peuvent être employées pour l'envoi de MCC par la poste ou par messagerie. Lorsque l'enveloppe intérieure contient du matériel cryptographique (quelle que soit sa classification) ou du MCC de niveau SECRET ou supérieur, la patte de fermeture et celle de l'enveloppe extérieure doivent être rabattues et collées à l'enveloppe puis recouvertes d'un ruban renforcé ou d'un ruban d'inviolabilité en guise de mesure de protection additionnelle.

Lorsque l'enveloppe intérieure contient du MCC de niveau inférieur ou égal à CONFIDENTIEL, les deux enveloppes peuvent être cachetées simplement en collant la patte de fermeture. Toutefois, si le gardien de sous-compte COMSEC craint que les enveloppes ne se déchirent en cours de route, il devrait les cacheter à l'aide d'un ruban renforcé ou d'un ruban d'inviolabilité.

10.7.4.2 Colis

Les colis contenant du MCC doivent être emballés dans du papier brun de bonne qualité et scellés à l'aide d'un ruban de papier renforcé de fibres. Le conditionnement des colis doit présenter les caractéristiques suivantes :

- tous les joints de l'emballage intérieur doivent être maintenus par du ruban de papier renforcé de fibres;
- les coins doivent être renforcés ou recouverts de carton pour éviter d'endommager l'emballage intérieur durant le transport;
- l'emballage extérieur doit être constitué de papier et de ruban renforcé de fibres suffisamment épais pour former un colis solide.

10.7.4.3 Boîtes de carton

Des boîtes en carton peuvent être employées comme contenant intérieur ou extérieur d'un colis. Les boîtes en carton usagées doivent être en bon état, et toutes les mentions antérieures doivent avoir été oblitérées. Il faut conditionner de façon à empêcher tout déplacement du contenu. Du ruban de papier renforcé de fibres doit servir à sceller tous les joints et à renforcer les arêtes ainsi que les coins.

10.7.4.4 Caisses en bois ou coffres de transport

Généralement, les caisses en bois et les coffres de transport ne devraient servir que d'emballage extérieur aux fins d'expédition, sauf lorsqu'ils sont spécialement conçus et autorisés pour servir d'emballage intérieur. Il faut entourer la caisse ou le coffre extérieur d'au moins un feuillard dans le sens de la longueur et d'un autre dans le sens de la largeur, au centre dans les deux cas. L'attache servant à fixer le feuillard dans le sens de la longueur doit se trouver au-dessus du feuillard posé dans le sens de la largeur.

10.7.4.5 Sacs de toile

Un sac de toile peut servir d'emballage extérieur pour un colis. Le sac doit être cacheté au moyen d'une fermeture à levier et d'un scellé (de modèle Plik). Le numéro d'identification de chaque scellé Plik est un mécanisme d'inviolabilité qui doit être utilisé aux fins de détection d'accès non autorisé au sac.

L'utilisateur doit prendre en note le numéro d'identification unique du scellé Plik lorsque celui-ci est utilisé pour sécuriser le sac. Lorsque le sac doit être ouvert, l'utilisateur doit confirmer que le numéro d'identification du scellé Plik sur le sac est le même. Cette vérification du numéro d'identification vise à confirmer que le sac n'a pas été ouvert par quelqu'un, puis fermé de nouveau au moyen d'un scellé Plik différent. Les coutures du sac doivent être à l'intérieur. Il ne faut pas utiliser de sac endommagé ou réparé.

10.7.4.6 Porte-documents

Au Canada, un porte-documents muni d'une serrure approuvée par le GC peut servir d'emballage extérieur pour du MCC devant être livré par un service de messagerie privé et autorisé. Prière de consulter le guide G1-001 de la GRC pour plus de détails.

10.7.5 Articles cryptographiques contrôlés

La préparation et l'emballage des CCI doivent répondre aux exigences suivantes :

- l'emballage des CCI non mis à la clé doit présenter les caractéristiques énoncées ci-dessous :
  - offrir une protection adéquate contre les dommages,
  - fournir les preuves permettant de cerner toute tentative d'ouverture du colis pendant que le matériel est en transit;
- afin de dissimuler la nature sensible du colis, les emballages contenant des CCI ne doivent pas porter la mention CCI ou une description (nomenclature) de l'équipement expédié; pour la documentation à l'extérieur du contenant, les CCI sont considérés comme des articles sensibles et contrôlés;
- les CCI doivent être expédiés uniquement à des destinations autorisées; les colis doivent être adressés de façon à assurer la livraison du matériel à une personne qui a été désignée au sein de l'organisation pour accepter la garde du matériel; le nom de la personne ne doit pas être inscrit dans l'adresse; il faut plutôt utiliser une désignation fonctionnelle (p. ex. un symbole de bureau ou un numéro de compte COMSEC du SNCMC).

10.8 Moyens de transport autorisés

10.8.1 Généralités

Les moyens de transport approuvés pour le MCC canadien sont énumérés dans le Tableau 6 – *Moyens de transport autorisés pour le matériel COMSEC comptable*.

10.8.2 Matériel COMSEC comptable de l'Organisation du Traité de l'Atlantique Nord et de l'étranger

Les moyens de transport approuvés faisant l'objet de la présente section ne s'appliquent pas au MCC classifié ni aux clés NON CLASSIFIÉ qui portent la mention CRYPTO de l'OTAN ou d'un pays étranger. Ce MCC doit être transporté conformément aux exigences de l'OTAN et du pays étranger.

NOTA : Prière de communiquer avec le CCIC concernant l'expédition de MCC à l'OTAN ou à des organismes étrangers.

10.8.3 Matériel COMSEC comptable de l'OTAN ou de l'étranger portant la mention UNCLASSIFIED, RESTRICTED ou U/FOUO (autre que les clés marquées CRYPTO)

Le MCC de l'OTAN et de l'étranger UNCLASSIFIED, RESTRICTED et U/FOUO (autre que les clés marquées CRYPTO) doit être expédié selon les moyens décrits dans le Tableau 6, lesquels ont été approuvés pour le MCC de niveau PROTÉGÉ A du même type. Qu'ils soient d'origine nationale ou étrangère, les CCI doivent toujours être expédiés selon les moyens de transport énoncés dans le Tableau 6.

10.9 Exigences relatives à la séparation

10.9.1 Généralités

Afin de réduire la possibilité de compromission des systèmes de communication et de l'équipement cryptographique, certains types de MCC ne sont jamais emballés ni transportés ensemble. Des emballages distincts mais faisant partie d'un même envoi (envois de colis multiples) ne permettent pas une séparation suffisante. Ainsi, non seulement le MCC doit-il être emballé séparément, mais il doit également être acheminé dans des envois distincts, sauf lorsque le CCIC en décide autrement par voie d'autorisation spéciale. Les gardiens de sous-compte COMSEC doivent respecter les règles de séparation qui suivent lors de l'emballage et de la transmission du MCC.

10.9.2 Clés

Les clés **ne doivent pas** être emballées ni expédiées avec l'équipement cryptographique connexe, sauf si les exigences énoncées à la section 10.4 sont respectées.

10.9.3 Équipement cryptographique mis à la clé

L'équipement cryptographique **ne doit pas** être emballé ni expédié en état mis à la clé (clé chargée dans l'équipement [avec ou sans CIK et NIP connexe]) sans l'autorisation du CCIC.

10.9.4 Documentation ou avis sur l'état des clés

La documentation ou les avis sur l'état des clés, qui révèlent la date et l'heure d'entrée en vigueur ou toute autre information pertinente concernant les clés doivent être emballés et expédiés séparément des autres formes de MCC ou de correspondance.

10.9.5 Matériel COMSEC non comptable

Le matériel COMSEC non comptable doit être expédié par les moyens approuvés correspondant à sa classification.

Lorsque du matériel COMSEC comptable et non comptable est expédié dans un même colis, il faut prendre soin de les identifier séparément l'un de l'autre. Seul le MCC doit figurer dans le *rapport de matériel COMSEC* inclus avec l'envoi. Un reçu distinct doit être inclus pour le matériel COMSEC non comptable.

10.10 Messagers autorisés à transporter du matériel COMSEC comptable

10.10.1 Messagers autorisés de l'entreprise du secteur privé

Les employés d'une entreprise privée qui détiennent l'habilitation de sécurité appropriée et qui ont été autorisés par le CCIC peuvent être employés comme messagers. Prière de communiquer avec le CCIC pour plus de détails sur les exigences auxquelles doivent satisfaire les membres du personnel nommés comme messagers.

10.10.2 Ordre de mission de messager COMSEC

L'*Ordre de mission de messager COMSEC* sert à confirmer à toutes les personnes concernées (p. ex. agents de sécurité des transporteurs aériens, agents des douanes) que le contenant ou colis scellé contient uniquement du matériel officiel. La présentation de l'*ordre de mission* devrait garantir, au matériel officiel transporté ou escorté par le messager, l'immunité contre toute forme de perquisition ou d'examen. Lorsque de plus amples mesures sont nécessaires pour vérifier l'authenticité d'un *ordre de mission de messager COMSEC*, le messager doit inviter le personnel intéressé à communiquer avec le CCIC.

10.10.3 Consignes à l'intention des messagers

L'ASE doit fournir au messager des consignes écrites qui décrivent les responsabilités que ce messager doit assumer pour être en mesure de garantir la protection du MCC jusqu'à ce que celui-ci ait été remis au destinataire. Les consignes au messager doivent comprendre, au minimum, les mesures suivantes :

- avant le départ, communiquer avec les représentants de la sécurité du transport aérien ou des douanes pour obtenir un dédouanement sans inspection;
- pendant le contrôle de sûreté préalable à l'embarquement ou l'inspection douanière, s'assurer que le MCC n'est ni compromis ni endommagé (p. ex. montrer l'*Ordre de mission de messager COMSEC* à la demande d'une autorité compétente);
- pour l'entreposage du matériel, fournir le nom des personnes avec qui communiquer advenant une urgence, un retard prolongé ou un arrêt en cours de route;
- fournir le nom des personnes avec qui le messager doit communiquer en cas de perte ou encore de compromission réelle ou soupçonnée du MCC.

10.11 Inspections douanières et préalables à l'embarquement

Dans les situations où un agent des douanes demande ou exige de voir le contenu d'un colis COMSEC, le messager autorisé ou, s'il y a lieu, le gardien de sous-compte COMSEC doit demander une entrevue avec l'agent supérieur des douanes ou avec le responsable de la sûreté du transport aérien. Le messager peut accepter de se soumettre à cette inspection limitée afin d'assurer aux agents des douanes que l'envoi ne contient rien d'autre que ce qui est inscrit dans la documentation. Chaque fois qu'un colis COMSEC fait l'objet d'une plus grande attention, le messager autorisé doit demander que l'inspection réponde aux conditions suivantes :

- être effectuée dans un endroit privé;
- être menée par des personnes dûment autorisées en présence du messager autorisé;
- se limiter à une visualisation extérieure du MCC.

Il est possible que le messager soit obligé d'interrompre la livraison et qu'il doive rapporter le MCC au point de départ s'il ne peut pas en venir à une entente relativement à l'étendue de l'inspection de dédouanement.

NOTA : Les radiographies sont autorisées, le cas échéant.

10.12 Transporteurs commerciaux

Un service de transport commercial (y compris le service des messageries prioritaires de Postes Canada) peut également assurer le service de messagerie pour du MCC (aux niveaux précisés dans le Tableau 6), à la condition que le transporteur fournisse une chaîne de responsabilité continue et qu'il assure la garde du matériel pendant le transit.

Il doit également offrir un service rapide (p. ex. livraison le lendemain), la protection physique ainsi que des fonctions de suivi et de localisation.

Lorsque le CCIC l'autorise, un transporteur commercial peut être appelé à transporter des CCI, à condition de s'engager par écrit à assurer les services suivants :

- service porte à porte et garantie de la livraison dans un délai raisonnable (en jours) selon la distance à parcourir;
- système manuel ou électronique de suivi des envois individuels de façon à ce que le transporteur puisse, dans les 24 heures suivant un avis, fournir des renseignements concernant le dernier emplacement connu d'un colis perdu;
- garantie de l'intégrité du contenu des colis, y compris la protection contre les dommages, le trafiquage et le vol;
- capacité d'entreposer les colis COMSEC en transit dans un endroit sûr et verrouillé (p. ex. cage de sécurité) auquel seul le personnel autorisé du transporteur peut accéder, dans les cas où le transporteur doit faire un arrêt prolongé à l'un de ses terminaux (durant les arrêts de nuit);
- signatures manuelles ou électroniques, chaque fois qu'un envoi change de main au sein de l'entreprise de transport;
- signatures horodatées au ramassage et à la livraison.

10.13 Réception du matériel COMSEC comptable

Un envoi de MCC adressé au nom du gardien de sous-compte COMSEC devrait être scellé au moment d'être remis au destinataire. Si la couverture ou l'emballage extérieur a été accidentellement ouvert par le personnel de la salle du courrier de l'entreprise, mais que la couverture ou l'emballage intérieur est demeuré intact et qu'il n'y a aucun signe de trafiquage, on juge alors qu'il n'y a pas eu d'incident COMSEC ni d'infraction à la sécurité. Toutefois, la couverture ou l'emballage extérieur ouvert par inadvertance doit être remis au gardien de sous-compte COMSEC avec le colis. Prière de consulter l'Annexe B pour les instructions détaillées concernant la réception du MCC.

Tableau 6 – Moyens de transport autorisés pour le matériel COMSEC comptable

Destination	Niveau de classification ou de protection du MCC (voir la légende du matériel COMSEC)				
	1, 2	**3, 4, 5**	**6, 7**	**8**	**9**
Au Canada	A, B, C (remarques I, II, IV)	A, B, C, D (remarques I, II, IV)	A, B, C, D, E, F (remarques I, II, IV)	A, B, D, E, F	A, B, C, D, E, F (remarques I, II)
Entre des adresses canadiennes à l'extérieur du Canada (voir la remarque V)	A, B, C (remarques I, II, IV)	A, B, C, D (remarques I, II, IV)	A, B, C, D (remarques I, II, IV)	A, B, D, E, F	A, B, C, D, E, F (remarques I, II)
À destination ou en provenance d'adresses non canadiennes (voir la remarque VI)	A, B, C (remarques I, II, IV)	A, B, C, D (remarques I, II, III, IV)	A, B, C, D (remarques I, II, III, IV)	A, B, D, E	A, B, C, D (remarques I, II, III)

Le MCC NON CLASSIFIÉ peut être expédié par n'importe quel moyen susceptible d'en assurer la livraison à destination en toute sécurité.
Le MCC NON CLASSIFIÉ portant la mention CRYPTO doit être expédié selon les critères s'appliquant au matériel PROTÉGÉ A (remarque IV).

Légende du matériel COMSEC	
1	Tout le MCC TRÈS SECRET et PROTÉGÉ C
2	Toute clé non emballée dans un conditionnement protecteur
3	Information cryptographique classifiée (autre que TRÈS SECRET)
4	Équipement cryptographique classifié
5	Clé SECRET emballée dans un conditionnement protecteur
6	Information COMSEC PROTÉGÉ B, CONFIDENTIEL et SECRET
7	Clé CONFIDENTIEL et PROTÉGÉ B emballée dans un conditionnement protecteur
8	CCI NON CLASSIFIÉ et matériel cryptographique NON CLASSIFIÉ
9	MCC PROTÉGÉ A

Légende des moyens autorisés	
A	Service du courrier diplomatique du gouvernement canadien
B	Messagers autorisés par le ministère
C	Transfert électronique
D	Messagers autorisés par l'entreprise du secteur privé
E	Transporteurs commerciaux autorisés
F	Service des messageries prioritaires de Postes Canada

Remarques :

I	Systèmes de transfert électronique du MCC autorisés au cas par cas par le CCIC.
II	Transfert électronique de clé s'il est autorisé par le CCIC et conformément à la doctrine opérationnelle du système.
III	Messagers du ministère ou de l'entreprise du secteur privé autorisés par le CCIC pour les urgences seulement.
IV	Le MCC de l'OTAN et de l'étranger (y compris les clés cryptographiques) peut nécessiter des considérations supplémentaires. Prière de communiquer avec le CCIC pour obtenir des instructions.
V	Concerne les adresses hors du Canada où le courrier et les envois de matériel, une fois livrés, sont manipulés et ouverts par des citoyens canadiens (pouvant avoir une double nationalité), notamment le personnel des bases des Forces canadiennes, des ambassades du Canada ou des bureaux consulaires. Prière de communiquer avec le CCIC pour obtenir des instructions.
VI	Concerne tout autre destinataire étranger non visé par la remarque V. Prière de communiquer avec le CCIC pour obtenir des instructions.

Instructions : Repérer le bon niveau de classification ou de protection du MCC à partir de la légende du matériel COMSEC. Trouver la destination dans la colonne supérieure gauche. Les moyens de transport autorisés sont indiqués par des lettres qui correspondent aux lettres énumérées dans la légende des moyens autorisés. Voir les remarques pour de plus amples renseignements.

11 Manutention et utilisation du matériel COMSEC comptable

11.1 Clés cryptographiques

11.1.1 Objet et utilisation

À moins d'indication contraire de l'autorité de contrôle (CA) – par l'entremise du CCIC –, les clés peuvent être utilisées uniquement pour les fins prévues, et ce, dans l'équipement cryptographique pour lequel elles ont été produites.

11.1.2 États de clé (ROUGE et NOIR)

Les clés sont développées, distribuées et manutentionnées dans l'un des deux états suivants : ROUGE (non chiffré) ou NOIR (chiffré). Les clés à l'état ROUGE sont comptabilisées au sein du SNCMC, tandis que les clés à l'état NOIR font l'objet d'un suivi en dehors du SNCMC.

11.1.3 Étiquettes

Exception faite des étiquettes apposées à l'installation de production, aucune autre étiquette ne peut être appliquée au conditionnement protecteur d'une clé, à moins que les Services à la clientèle en matière de COMSEC ne l'aient autorisé.

11.1.4 Conditionnement protecteur

Certaines clés sont emballées dans un conditionnement protecteur au moment de leur production. Dans la plupart des cas, ce conditionnement ne sera ouvert qu'au moment où l'article est remis au titulaire de prêts ou à l'utilisateur autorisé. Il faut inspecter le conditionnement protecteur à la réception initiale, durant l'inventaire, avant une remise et avant la destruction de la clé scellée afin de détecter, le cas échéant, tout signe de trafiquage.

NOTA 1 : Le conditionnement protecteur recouvrant des clés TRÈS SECRET doit être retiré selon les contrôles TPI.

NOTA 2 : Le conditionnement protecteur (p. ex. les distributeurs de clés) n'est pas considéré comme un emballage intérieur (voir la section 10.7.2).

11.1.4.1 Clés électroniques sur support de stockage amovible magnétique ou optique

Le gardien de sous-compte COMSEC doit s'assurer que le conditionnement protecteur du SSA magnétique ou optique servant à la distribution de clés électroniques demeure intact jusqu'à l'utilisation du SSA en question.

11.1.4.2 Clés électroniques sur un dispositif de stockage de clés

Le gardien de sous-compte COMSEC doit s'assurer que le conditionnement protecteur d'une clé de diversification électronique ou d'une clé opérationnelle électronique qui a été reçue sur un KSD demeure intact jusqu'à ce que la clé soit utilisée. Habituellement attachée à un KSD, l'étiquette contient de l'information permettant de reconnaître la clé électronique. Le KSD étiqueté est scellé dans un sac en plastique ou dans une pellicule thermoplastique.

11.1.5 Copies de clé

11.1.5.1 Clés symétriques opérationnelles

Des copies d'une clé opérationnelle peuvent être créées, en tout ou en partie, avec l'autorisation de l'AC et conformément aux prescriptions énoncées dans la doctrine liée à l'équipement. Il conviendra, notamment, d'appliquer les règles suivantes :

- conserver le titre abrégé de la clé faisant l'objet d'une copie;
- protéger les copies conformément à leur classification et à la mention CRYPTO, le cas échéant;
- ne pas conserver les copies au-delà de la date de destruction de la clé d'origine (mais elles peuvent être détruites avant cette date);
- détruire toutes les copies avant de détruire la clé d'origine;
- comptabiliser localement les copies à l'aide d'un système de suivi manuel, lorsque les pistes de vérification de l'équipement ou du système ne sont pas disponibles.

11.1.5.2 Clés symétriques de test

Les clés de test peuvent être copiées et comptabilisées au sein d'un compte COMSEC comme des articles CC 4 ou CC 7. Lorsqu'une clé de test est transférée à un autre compte COMSEC, toutes les copies connexes doivent être détruites.

11.1.5.3 Clés asymétriques

Il est interdit de faire des copies d'une clé asymétrique.

11.2 Équipement cryptographique

11.2.1 Vérification visuelle

Le gardien de sous-compte COMSEC doit vérifier si l'équipement cryptographique (classifié ou non classifié et CCI) est complet au moment de sa réception initiale, durant la prise d'inventaire et au moment de sa remise.

11.2.2 Étiquettes de l'équipement

Les seules étiquettes approuvées pouvant être jointes à l'équipement cryptographique ou à son conditionnement protecteur sont les suivantes :

- une étiquette du fabricant;
- une plaque de nomenclature d'équipement;
- une étiquette CCI;
- une ou plusieurs étiquettes d'inviolabilité;
- toute autre étiquette approuvée par le CST.

Une étiquette approuvée ne doit jamais être couverte (p. ex. par une autre étiquette) ni enlevée, à moins d'une autorisation expresse du CST. Tout signe visible de trafiquage des étiquettes doit être signalé, tel qu'il est décrit à la section 16. Lorsque le gardien n'est pas certain s'il s'agit réellement d'un incident COMSEC, il doit communiquer avec le CCIC pour obtenir de l'assistance.

11.2.3 Modification

Aucune modification (y compris l'ajout d'étiquettes) ne peut être apportée à l'équipement cryptographique sans l'approbation préalable du CCIC. Seuls les membres du personnel autorisé et qualifié peuvent effectuer les modifications approuvées sur l'équipement cryptographique.

11.2.4 Équipement cryptographique installé à des fins opérationnelles

Le gardien de sous-compte COMSEC doit veiller à l'application des mesures suivantes :

- tous les utilisateurs de l'équipement lisent et comprennent la doctrine portant sur l'équipement;
- l'équipement installé à des fins opérationnelles est protégé en fonction de sa classification ou de celle des clés, selon le niveau le plus élevé;
- les procédures autorisées sont mises en place pour empêcher l'utilisation non autorisée de l'équipement ou l'extraction des clés qu'il contient.

11.2.5 Équipement cryptographique classifié – Mis à la clé et non surveillé

L'équipement cryptographique classifié qui est mis à la clé et utilisé sans surveillance peut être exploité uniquement dans une zone de haute sécurité dotée des mêmes contrôles supplémentaires que les clés TRÈS SECRET. Les contrôles TPI et NLZ ne sont pas requis, sauf lorsqu'une clé TRÈS SECRET est utilisée.

11.2.6 Articles cryptographiques contrôlés

11.2.6.1 Généralités

Bien qu'ils soient non classifiés par définition, les CCI sont néanmoins contrôlés. Lorsqu'un CCI est mis à la clé, il hérite du niveau de classification de la clé utilisée. Sauf si le CCIC l'autorise (voir la section 9.6.2), les CCI doivent être mis à zéro avant leur entreposage ou leur livraison.

Des contrôles minimaux s'appliquent aux CCI lorsque ces derniers correspondent à ce qui suit :

- CCI non mis à la clé;
- CCI installés et mis à la clé avec une clé non classifiée;
- CCI mis à la clé avec une clé classifiée ou protégée.

Les dispositions ci-dessous s'appliquent aux CCI installés à des fins opérationnelles. Pour obtenir des instructions détaillées sur la sécurité des CCI, prière de consulter la doctrine de l'équipement concerné ou de communiquer avec le CCIC.

11.2.6.2 Articles cryptographiques contrôlés non mis à la clé

Il incombe à l'entreprise du secteur privé qui détient un CCI d'appliquer des contrôles adéquats sur le plan de la sécurité physique et des procédures pour empêcher le retrait non autorisé du CCI ou de ses composants.

11.2.6.3 Articles cryptographiques contrôlés installés et mis à la clé avec une clé non classifiée

- **Sous surveillance :** L'entreprise du secteur privé est responsable d'empêcher le personnel non autorisé d'accéder aux CCI. Pour ce faire, elle doit utiliser des contrôles physiques ou affecter du personnel autorisé à la surveillance d'éventuelles tentatives d'accès.

- **Sans surveillance :** Les CCI laissés sans surveillance doivent, au minimum, être exploités dans une zone de travail. L'entreprise du secteur privé est responsable d'empêcher le personnel non autorisé d'accéder aux CCI en appliquant des contrôles physiques adéquats (p. ex. des salles verrouillées, des alarmes ou des vérifications ponctuelles).

11.2.6.4 Articles cryptographiques contrôlés installés et mis à la clé avec une clé classifiée ou protégée

- **Sous surveillance :** Les CCI mis à la clé doivent être assujettis au contrôle strict et permanent de membres du personnel de l'entreprise qui possèdent une habilitation de sécurité de niveau égal ou supérieur au niveau de classification de la clé utilisée. Dans le cas d'une clé TRÈS SECRET, les contrôles NLZ doivent être appliqués, sauf si la clé réside sous forme électronique et à l'état NOIR dans l'équipement cryptographique (p. ex. les dispositifs SCIP) ou lorsque l'équipement a été modifié de façon à empêcher qu'une personne seule accède à cette clé.
- **Sans surveillance :** Les CCI mis à la clé peuvent être exploités uniquement dans une zone de haute sécurité dotée des mêmes contrôles supplémentaires que ceux appliqués à la mise à la clé TRÈS SECRET. Les contrôles TPI et NLZ ne sont pas requis, sauf lorsqu'une clé TRÈS SECRET est utilisée.

11.2.7 Équipement de stockage de clés ou de remplissage contenant une clé

11.2.7.1 Dispositifs communs de remplissage contenant des clés à l'état ROUGE

Les dispositifs communs de remplissage (p. ex. KYK-13) dans lesquels sont stockées des clés à l'état ROUGE et qui ne fournissent aucun enregistrement de transaction ne doivent pas être utilisés à des fins de stockage à long terme. Les clés peuvent rester dans ce type de dispositif pendant une période maximale de 12 heures après la fin de la cryptopériode. Ce type de dispositif doit être marqué de façon à indiquer le niveau de classification le plus élevé des clés qui y sont stockées et doit être conservé selon les contrôles TPI quand il contient des clés TRÈS SECRET.

11.2.7.2 Dispositifs de gestion de palier 3 contenant des clés à l'état NOIR

Les dispositifs de gestion de palier 3 (T3MD pour *Tier 3 Management Device*) dans lesquels sont stockées des clés à l'état NOIR doivent être utilisés conformément à la doctrine de l'équipement concerné.

11.2.7.3 Support de stockage amovible magnétique ou optique contenant des clés

Les SSA magnétiques et optiques contenant des clés à l'état ROUGE doivent être retournés dans un contenant sécurisé après que les clés ou les données connexes ont été chargées dans l'unité cryptographique de destination (ECU pour *End Cryptographic Unit*). Les SSA contenant des clés à l'état ROUGE doivent être marqués de façon à indiquer le niveau de classification le plus élevé des clés qu'ils contiennent et, au besoin, ils doivent porter la mention CRYPTO.

NOTA : Les SSA comprennent les cédéroms, les DVD et tous les autres supports optiques, les clés USB à mémoire flash, les cartes mémoire ainsi que tous les autres supports magnétiques.

11.2.7.4 Réutilisation de supports de stockage amovibles magnétiques et optiques non comptables

Un SSA non comptable utilisé pour le transfert de clés à l'état NOIR peut être réutilisé une fois que les clés à l'état NOIR ont été retirées et que le SSA a été nettoyé de façon appropriée (voir l'ITSG-06, *Effacement et déclassification des supports d'information électroniques*, pour obtenir de plus amples détails sur la déclassification et le nettoyage des SSA).

11.2.8 Pistes de vérification de l'équipement

11.2.8.1 Responsabilité liée à l'examen

Sauf pour les pistes de vérification de T3MD, lesquelles doivent être téléversées au CCIC aux fins d'examen et de conservation, le gardien de sous-compte COMSEC est responsable de s'assurer que les pistes de vérification de l'équipement cryptographique approuvé par le CST sont examinées, tel qu'il est indiqué dans la doctrine connexe et tel qu'il est exigé par le CCIC.

11.2.8.2 Examen des pistes de vérification

La personne autorisée à examiner les données des pistes de vérification doit assumer les responsabilités suivantes :

- ne pas être le principal utilisateur de l'équipement cryptographique;
- répondre aux exigences en matière d'accès COMSEC énoncées à la section 8.1;
- avoir suffisamment de connaissances relativement à l'utilisation de l'équipement cryptographique et des clés qui y sont stockées ou qui y ont été chargées;
- confirmer que seules des copies autorisées des clés ont été créées;
- pouvoir détecter les anomalies présentes dans les données des pistes de vérification;
- transmettre les résultats de l'examen des pistes de vérification au gardien de sous-compte COMSEC, qui en transmettra ensuite un exemplaire au CCIC.

11.2.8.3 Conservation des journaux de vérification

Les journaux de vérification doivent être conservés conformément à la section 5.2.5, à la doctrine de l'équipement concerné – lorsque les dispositions diffèrent de la présente directive –, ou aux directives du CCIC.

11.2.8.4 Conservation des registres et des pistes de vérification

Le gardien de sous-compte COMSEC doit conserver un registre des examens de piste de vérification jusqu'à ce que le sous-compte COMSEC reçoive un *avis de rapprochement d'inventaire périodique* attestant que son inventaire a été rapproché.

11.3 Publications COMSEC

11.3.1 Reproduction

Les publications COMSEC comptables ne doivent pas être reproduites, à moins que leur reproduction soit autorisée en vertu d'un contrat que le secteur privé conclut directement avec le CCIC ou par l'intermédiaire de SPAC. Prière de consulter l'ITSD-08 pour de plus amples renseignements.

11.3.2 Vérification des pages

11.3.2.1 Exigence

Le gardien de sous-compte COMSEC (ou toute autre personne autorisée) doit vérifier les pages des publications COMSEC comptables non scellées afin de s'assurer que toutes les pages requises sont présentes. Pour effectuer la vérification des pages, il faut vérifier la présence de chaque page par rapport à la « Liste des pages en vigueur » ou des « Instructions relatives au traitement », selon le cas.

NOTA : Une vérification de pages doit être effectuée à la réception initiale d'une publication COMSEC comptable (notamment la réception par un titulaire de prêts et le gardien de sous-compte COMSEC d'une publication retournée).

11.3.2.2 Fréquence

Les pages des publications COMSEC comptables et des modificatifs de publications COMSEC comptables doivent être vérifiées selon les échéances suivantes :

- durant chaque inventaire de sous-compte COMSEC;
- au moment de la réception;
- avant un transfert ou une remise;
- avant une destruction courante;
- lorsqu'un gardien de sous-compte COMSEC sortant n'est pas disponible pour produire un *rapport d'inventaire*;

  NOTA : Le gardien de sous-compte COMSEC entrant et un témoin doivent effectuer une vérification de pages de toutes les publications COMSEC comptables.
- au moment de l'inventaire visuel et avant la signature du *Rapport de possession*;
- après la publication d'un modificatif (y compris le retrait ou le remplacement de pages).

11.3.2.3 Aucune page manquante

Lorsqu'aucune page ne manque, il faut signer et dater la page « Registre des pages vérifiées ». Lorsque la publication COMSEC comptable n'inclut pas cette page, il faut signer et dater la page couverture.

11.3.2.4 Pages manquantes

S'il manque des pages, la page « Registre des pages vérifiées » doit être annotée en conséquence, et un *Rapport d'incident COMSEC* doit être présenté conformément à la section 16. Lorsque le gardien de sous-compte COMSEC reçoit du matériel COMSEC incomplet (pages manquantes) en provenance d'une installation de production, il doit en informer l'autorité compétente et lui demander la marche à suivre (p. ex. retourner le matériel aux fins de remplacement, détruire le matériel ou l'utiliser même s'il manque des pages).

11.3.2.5 Pages en double

S'il y a des pages en double, le gardien de sous-compte COMSEC doit établir un *Rapport de possession* (GC-223) conformément à la section 7 et demander au CCIC la marche à suivre pour l'élimination des pages en double. Le *Rapport de possession* doit énumérer le numéro de page à même le titre abrégé (p. ex. AMSG 600, page 3) et le numéro de comptabilité attribué au matériel. Il faut inscrire les pages en double ainsi que l'élimination subséquente dans la page « Registre des pages vérifiées ».

11.3.3 Modificatifs

11.3.3.1 Modificatifs imprimés

Le gardien de sous-compte COMSEC doit comptabiliser un modificatif imprimé de la même manière qu'une publication COMSEC comptable, conformément à son CC, jusqu'à ce qu'il soit inséré et que l'information supprimée ou remplacée ait été détruite. Au moment d'établir le *Rapport de destruction* (GC-223), il doit veiller à y inscrire le titre abrégé, l'édition et le numéro de comptabilité du modificatif (et non ceux de la publication). Les modificatifs imprimés doivent être insérés l'un à la suite de l'autre. Si un modificatif a été reçu, mais que les modificatifs précédents n'ont pas été insérés, ceux-ci doivent être insérés (ou obtenus et insérés) avant le dernier modificatif.

11.3.3.2 Insertion des modificatifs

Les règles suivantes s'appliquent à l'insertion des modificatifs :

- le gardien de sous-compte COMSEC (ou toute autre personne autorisée) doit insérer le modificatif dans les plus brefs délais suivant sa réception (ou sa date d'entrée en vigueur);
- les membres du personnel autorisé à insérer des modificatifs doivent avoir été adéquatement formés;
- les instructions précises contenues dans la lettre de promulgation ou les instructions relatives au traitement doivent être lues et comprises avant l'insertion des modificatifs;
- un modificatif doit être intégralement inséré d'un coup et non progressivement;
- si des pages de remplacement sont comprises dans le modificatif, il faut procéder à une vérification des pages de la publication ainsi que de l'information à modifier avant de détruire celle-ci; la destruction par inadvertance de sections en vigueur des publications doit être signalée comme un **incident COMSEC**, conformément à la section 16;
- la personne qui insère un modificatif doit inscrire l'insertion de ce modificatif à la page « Registre des modificatifs »; si des pages ont été ajoutées à la publication ou enlevées de celle-ci, cette personne doit dater et signer la page « Registre des pages vérifiées »;
- tout membre du personnel – autre que le gardien de sous-compte COMSEC –, ayant inséré un modificatif doit retourner toutes les pages retirées ou remplacées au gardien de sous-compte COMSEC aux fins de destruction;
- les pages retirées ou remplacées doivent être mises dans une enveloppe scellée sur laquelle sont inscrits le titre abrégé, le numéro de comptabilité et la classification du modificatif;
- les pages retirées ou remplacées doivent être détruites dans les cinq jours ouvrables suivant l'insertion du modificatif;
- après qu'un modificatif a été inséré, un membre du personnel de garde, autre que la personne qui a inséré le modificatif, doit vérifier les pages de la publication.

11.4 Suivi local de matériel COMSEC non comptable

11.4.1 Système de suivi local

Le gardien de sous-compte COMSEC doit contrôler au moyen d'un système de contrôle et de suivi local tout matériel (p. ex. CIK, NIP, mots de passe, disques de configuration) associé à l'équipement cryptographique qui ne peut pas être contrôlé à l'aide du SNCMC. Le contrôle et la manutention de ce matériel doivent se conformer à la présente directive, sauf indication contraire provenant de la doctrine de l'équipement concerné, de l'autorité d'origine ou du CCIC.

11.4.2 Clés de contact cryptographiques

Le gardien de sous-compte COMSEC doit faire un suivi local des CIK au moyen d'une procédure qui réduit au minimum toute compromission possible associée à leur utilisation. Les procédures de suivi local des CIK doivent inclure ce qui suit :

- enregistrer chaque création de CIK, en prenant soin de noter le numéro de série de la CIK (dans la mesure du possible), le numéro de série et l'emplacement de l'équipement connexe, la date à laquelle l'équipement a été mis à la clé et le nom de chaque titulaire de prêts autorisé à utiliser la CIK;
- s'assurer que chaque CIK a fait l'objet d'un accusé de réception signé par le titulaire de prêts et confirmer au moins une fois par année que chaque titulaire de prêts détient toujours sa CIK;
- expédier les CIK (séparément de l'équipement connexe) par l'une des voies COMSEC approuvées par le CCIC;
- fournir un moyen d'entreposage adéquat pour une CIK qui n'est pas sous le contrôle personnel du titulaire de prêts;
- mettre à zéro ou détruire les CIK qui ne sont plus requises;
- élaborer des procédures permettant de détecter les compromissions possibles.

11.4.3 Numéros d'identification personnels et mots de passe

Lorsqu'il doit conserver un enregistrement écrit ou une liste principale des NIP ou des mots de passe, le gardien de sous-compte COMSEC doit veiller à la réalisation de ce qui suit :

- chaque enregistrement comprend le nom et le numéro de téléphone de la ou des personnes connaissant le NIP ou le mot de passe, le numéro de série et l'emplacement de l'équipement connexe, ainsi que la date à laquelle le NIP ou le mot de passe a été changé;
- chaque enregistrement de NIP et de mot de passe est protégé conformément à sa classification ou à la classification de l'équipement connexe, selon le niveau le plus élevé;
- l'accès à un NIP ou à un mot de passe individuel est limité à la personne à qui il a été attribué, à moins qu'une situation d'urgence ne dicte le contraire;
- les enregistrements de NIP ou de mot de passe de même que les NIP et les mots de passe individuels, sont distribués par les voies COMSEC ou selon les méthodes approuvées pour le matériel classifié.

11.4.3.1 Changement des numéros d'identification personnels et des mots de passe

Le gardien de sous-compte COMSEC doit veiller à ce que les NIP et les mots de passe liés à l'équipement cryptographique soient changés, tel qu'il est décrit dans la doctrine portant sur l'équipement. À moins d'indication contraire, le NIP ou le mot de passe doit être changé dans les cas suivants :

- lorsque l'équipement est mis en service pour la première fois par le gardien de sous-compte COMSEC;
- lorsqu'une personne qui connaît le NIP ou le mot de passe n'est plus autorisée à accéder à l'équipement;
- lorsqu'une personne non autorisée a eu accès à l'enregistrement écrit du NIP ou du mot de passe;
- lorsque le NIP ou le mot de passe a été effectivement ou présumément compromis;
- lorsque le NIP ou le mot de passe n'a pas été changé depuis six mois ou plus.

11.4.3.2 Rangement des numéros d'identification personnels et des mots de passe

Lorsqu'ils doivent être conservés, les enregistrements de NIP ou de mot de passe de même que la liste de NIP et de mots de passe doivent être protégés et gérés par l'autorité appropriée (l'ACM du CCIC ou le gardien COMSEC du CCIC), qui devra les marquer et les protéger conformément au niveau de classification le plus élevé du matériel protégé par le NIP ou le mot de passe.

11.4.4 Disques de configuration

Le gardien de sous-compte COMSEC doit faire en sorte que l'étiquette apposée à chaque disque de configuration d'équipement permette de reconnaître l'équipement auquel il appartient et indique la date de création ainsi que la classification. Un mode de suivi local doit permettre l'enregistrement de l'information figurant sur l'étiquette, le nom de la personne en contrôle du disque et l'emplacement de l'équipement connexe.

11.4.5 Mises à niveau logicielles

Toutes les versions logicielles doivent être approuvées par le CCIC. Le gardien de sous-compte COMSEC doit contrôler le processus de mise à niveau logicielle de l'équipement afin que tout l'équipement cryptographique opérationnel, y compris l'équipement gardé en réserve, demeure compatible. Toutes les mises à niveau obligatoires doivent être exécutées avant la date fixée par le CCIC.

NOTA : La réalisation des mises à niveau logicielles obligatoires est vérifiable. Par conséquent, le gardien de sous-compte COMSEC doit aviser les Services à la clientèle en matière de COMSEC une fois qu'il a effectué une telle mise à niveau.

12 Disposition du matériel COMSEC comptable

12.1 Exigences générales

Le MCC ne doit pas faire l'objet d'une disposition sans l'autorisation expresse du CCIC. La disposition du MCC peut être réalisée selon l'un des trois modes suivants : transfert, vente ou destruction.

NOTA : Le personnel qui procède à la destruction doit posséder une habilitation de sécurité égale ou supérieure au niveau de sensibilité le plus élevé du matériel COMSEC détruit, mais jamais inférieure au niveau SECRET.

12.2 Autorisation

À part les pages retirées ou remplacées, une entreprise du secteur privé ne peut détruire que les clés dont le CCIC a autorisé la destruction par voie d'une lettre indiquant, notamment, l'état du MCC. Lors de la destruction du MCC, l'autorisation de destruction doit être citée dans les documents et rapports COMSEC.

12.3 Destruction des clés

12.3.1 Généralités

Pour détruire des clés, il faut faire appel aux procédures, aux méthodes et aux dispositifs de destruction autorisés. Les entreprises du secteur privé doivent établir les procédures appropriées et fournir les ressources nécessaires à la destruction courante des clés, tel qu'il est expliqué dans la présente directive.

12.3.2 Non-disponibilité des dispositifs de destruction

Les clés qui ne peuvent être mises à zéro ou détruites au sous-compte COMSEC en raison de la non-disponibilité de dispositifs de destruction doivent être retournées au CCIC aux fins de destruction.

12.3.3 Clés remises aux fins d'utilisation

Les clés remplacées, qu'elles le soient régulièrement ou non, doivent être détruites dans les douze heures suivant leur remplacement, sauf dans les cas suivants :

- durant une période de congé prolongée ou lorsque les circonstances sont telles que la règle de douze heures ne peut être appliquée (p. ex. installation de destruction non opérationnelle), les clés doivent être détruites dans les plus brefs délais et ne devraient pas être conservées plus de 72 heures après leur remplacement;
- lorsque les dispositifs de destruction autorisés ne sont pas disponibles, les clés remplacées doivent être détruites dans les plus brefs délais suivant la fin des opérations;
- les KEK doivent être détruites dès qu'elles ont été chargées dans un équipement cryptographique, à moins que la doctrine portant sur l'équipement n'autorise leur conservation;
- les clés mises en cause dans des situations de compromission doivent être détruites dans les 72 heures suivant la réception des instructions relatives à leur disposition; dans ce cas, des *rapports de destruction* doivent être envoyés au CCIC immédiatement après leur destruction.

12.4 Destruction de l'équipement cryptographique, des publications, des supports de stockage amovibles et des clés matérielles comptables

En temps normal, l'équipement cryptographique, les publications, les SSA et les clés matérielles comptables (p. ex. les mémoires mortes programmables [PROM pour *Programmable Read-Only Memory*], les fiches de permutation et les aides de fabrication connexes) doivent être retournés au parrain du GC, aux fins de disposition.

12.5 Réalisation de la destruction courante des clés

12.5.1 Personnel

12.5.1.1 Gardien de sous-compte COMSEC et gardien suppléant

Le gardien de sous-compte COMSEC et le gardien suppléant effectuent normalement la destruction courante des clés. Cependant, il est préférable d'accorder le pouvoir de détruire les clés remplacées à d'autres membres du personnel qui ont l'habilitation de sécurité appropriée et qui ont pris part à une séance d'initiation COMSEC (et qui attesteront ensuite de la destruction auprès du gardien de sous-compte COMSEC) que de retarder la destruction, même pendant peu de temps.

12.5.1.2 Titulaire de prêts

Le gardien de sous-compte COMSEC peut accorder le pouvoir de détruire des clés à un titulaire de prêts qui dispose de l'équipement requis, à condition que la destruction ait lieu en présence d'un témoin ayant l'habilitation de sécurité appropriée et ayant reçu une séance d'initiation COMSEC. Dans les cas où un dispositif de destruction approprié n'est pas disponible, les clés doivent être retournées au gardien de sous-compte COMSEC aux fins de destruction.

12.5.1.3 Témoin

La destruction des clés sur des supports physiques qui n'offrent pas de piste de vérification doit être effectuée en présence d'un témoin autorisé.

NOTA 1 : Une personne ne peut signer à titre de témoin que dans la mesure où elle a vu la clé en question.

NOTA 2 : Il faut s'assurer que seule la clé autorisée à des fins de destruction est effectivement détruite.

12.5.2 Exigences relatives au personnel autorisé

Le gardien de sous-compte COMSEC doit veiller à ce que les personnes qu'il autorise à détruire des clés répondent aux critères suivants :

- satisfaire aux exigences d'accès au MCC et posséder une habilitation de sécurité correspondant au niveau de classification le plus élevé des clés à détruire;
- être informé des procédures appropriées de destruction.

12.5.3 Étapes de la destruction

Lorsqu'il s'agit de détruire des clés, les deux personnes autorisées doivent suivre les étapes suivantes :

1. s'assurer qu'une autorisation a été accordée pour les clés à détruire (voir la section 12.2) avant d'inscrire le matériel dans le *Rapport de destruction*;
2. inscrire tout le matériel à détruire dans le *Rapport de destruction* conformément à la section 7.4.5; utiliser le *Rapport de destruction* (non signé) (ou la fiche HI/DR ou tout autre registre de destruction local) comme « liste de contrôle » durant le processus de destruction, afin de s'assurer que le bon MCC sera détruit;
3. immédiatement avant la destruction, comparer le matériel à détruire (titre abrégé, édition, numéro de comptabilité et quantité de chaque article) à la liste figurant sur le *Rapport de destruction* (ou la fiche HI/DR ou tout autre registre de destruction local) et s'assurer que les renseignements comptables sont exacts;

4. détruire le matériel sans délai en utilisant les méthodes de destruction approuvées;
5. examiner le dispositif de destruction et la zone immédiate afin de s'assurer que tout le matériel a été détruit;
6. inspecter soigneusement le résidu afin de s'assurer que la destruction est complète;
7. signer (gardien et témoin) le *Rapport de destruction* (ou la fiche HI/DR ou tout autre registre de destruction local) à moins que la doctrine portant sur l'équipement ne précise qu'aucun témoin n'est nécessaire; il ne faut pas signer le *Rapport de destruction* tant que la destruction complète du matériel qui y est répertorié n'a pas été confirmée.

12.6 Méthodes de destruction courante

12.6.1 Généralités

Les critères de destruction énumérés dans les sections qui suivent s'appliquent aux clés comptables.

NOTA : En cas de doute quant à la conformité d'une méthode de destruction de clés aux normes minimales décrites ci-après, prière de communiquer avec le CCIC pour obtenir des conseils.

12.6.2 Incinération

Les clés sur bande papier doivent brûler intégralement (jusqu'à ce que la bande soit réduite en cendres blanches) dans un espace fermé (de sorte que rien n'échappe à la combustion). Il faut inspecter les cendres et, au besoin, les fragmenter.

12.6.3 Pulvérisation, hachage ou désintégration

Les dispositifs servant à pulvériser, à hacher ou à désintégrer les clés sur bande papier doivent réduire celles-ci en particules de rebut ne dépassant pas cinq millimètres (1/5 pouce) de largeur, toutes longueurs confondues.

12.6.4 Déchiquetage par coupe en travers

L'utilisation de déchiqueteuses de type II capable de réduire le matériel en morceaux qui ne dépassent pas 1,0 mm de largeur et 14,3 mm de longueur, permet d'obtenir une destruction « définitive » (prière de consulter le guide G1-001 de la GRC pour plus de détails).

12.6.5 Clés électroniques

La destruction des clés électroniques consiste à mettre à zéro ou à écraser les clés.

Pour des instructions précises sur la destruction ou la mise à zéro des clés électroniques chargées dans un équipement COMSEC comptable, prière de se reporter à la doctrine portant sur l'équipement ou de communiquer avec le CCIC.

12.6.6 Distributeurs en plastique

Il faut briser ou écraser les distributeurs vides afin de s'assurer que tous les segments de clé ont été retirés, puis les éliminer sous forme de déchets non classifiés.

13 Inventaire de sous-compte COMSEC

13.1 Motifs de l'inventaire

L'inventaire est la vérification des articles détenus par un sous-compte COMSEC. Le CCIC tient à jour une base de données dans laquelle est enregistré le matériel COMSEC comptable CC 1, CC 2, CC 4, CC 6 et CC 7 porté au sous-compte COMSEC. Les données proviennent des *rapports de matériel COMSEC* (p. ex. *rapports de destruction* ou *de possession*) que le sous-compte COMSEC transmet au CCIC. Les *rapports de matériel COMSEC* qui ont été traités par le sous-compte COMSEC, mais qui n'ont pas été entrés dans la base de données du CCIC, donneront lieu à des écarts entre la base de données du CCIC et les dossiers du sous-compte.

L'inventaire vise à s'assurer de ce qui suit :

- que les dossiers du sous-compte COMSEC sont à jour;
- que la base de données du CCIC est tenue à jour en veillant à ce que tous les *rapports de matériel COMSEC* ont bel et bien été envoyés au CCIC et qu'ils ont été traités par celui-ci;
- que le MCC porté au sous-compte COMSEC est bel et bien détenu par celui-ci et qu'il a été contrôlé à vue par le personnel autorisé;
- que le MCC porté au sous-compte COMSEC est toujours nécessaire.

13.2 Types d'inventaire

13.2.1 Inventaire périodique

Le gardien de sous-compte COMSEC et le gardien suppléant doivent procéder à un inventaire visuel périodique (au moins tous les 18 mois) de tout le MCC porté à leur sous-compte COMSEC (y compris le MCC que les titulaires de prêts ont en leur possession).

Le CCIC envoie, au gardien de sous-compte COMSEC, un *Rapport d'inventaire* (GC-223) qui rend compte de tout le MCC porté au sous-compte COMSEC à la date d'impression du rapport. Le gardien de sous-compte COMSEC et le gardien suppléant doivent ensuite procéder à un dénombrement visuel du matériel pour vérifier si l'inventaire correspond aux éléments figurant dans le rapport (voir la section 13.3.3 pour le matériel n'y figurant pas) et retourner le *Rapport d'inventaire* signé au CCIC dans les 10 jours ouvrables suivant la date de réception initiale du rapport.

13.2.2 Inventaire lors du changement de gardien de sous-compte COMSEC

Lorsqu'un gardien de sous-compte COMSEC part définitivement ou pour une durée non déterminée, la personne nouvellement nommée pour le remplacer doit procéder à l'inventaire visuel de tout le MCC détenu par le sous-compte COMSEC avant que le changement de gardien entre en vigueur officiellement.

Après avoir terminé la prise d'inventaire, le nouveau gardien de sous-compte COMSEC doit signer le *Rapport d'inventaire* à titre de gardien du sous-compte COMSEC. Le nouveau gardien de sous-compte COMSEC, exception faite des écarts à régler, assume dès lors la responsabilité de tout le MCC détenu au compte.

13.2.3 Inventaire spécial

Le gardien de sous-compte COMSEC doit procéder à un inventaire spécial lorsque le CCIC le lui demande. On peut demander la prise d'un inventaire spécial pour divers motifs, notamment la perte présumée d'un MCC ou de fréquentes dérogations aux procédures comptables.

Les procédures suivies dans le cadre d'un inventaire périodique (parfois appelé « inventaire annuel » dans d'autres documents) doivent être utilisées pour un inventaire spécial.

13.3 Rapports d'inventaire

13.3.1 Rapport d'inventaire initial

Le CCIC distribue un *Rapport d'inventaire initial* à tous les sous-comptes COMSEC pour annoncer le début du processus d'inventaire. Chaque *rapport d'inventaire* répertorie tous les articles COMSEC comptables CC 1, CC 2, CC 4, CC 6 et CC 7 qui, à la date d'impression du *Rapport d'inventaire*, sont enregistrés dans la base de données du CCIC pour chaque sous-compte COMSEC.

13.3.2 Rapports d'inventaire de sous-compte COMSEC

Les *rapports d'inventaire* produits par le gardien de sous-compte COMSEC peuvent s'adresser à deux lectorats différents :

- personnel du sous-compte COMSEC (utilisation durant le contrôle visuel du matériel en stock);
- personnel du CCIC (dresser l'inventaire intégral des articles détenus par le sous-compte COMSEC).

13.3.2.1 Distribution de rapports d'inventaire au sein du sous-compte COMSEC

Le gardien de sous-compte COMSEC prépare les *rapports d'inventaire* aux fins de distribution interne aux titulaires de prêts. Ces rapports énumèrent tous les articles COMSEC comptables CC 1, CC 2, CC 4, CC 6 et CC 7 que le gardien de sous-compte COMSEC a remis à des titulaires de prêts au sein du sous-compte ainsi que les articles qui sont toujours prêtés en dehors du sous-compte.

13.3.2.2 Distribution du rapport d'inventaire au Compte COMSEC industriel du CST

Le gardien de sous-compte COMSEC compile les résultats de tous les *rapports d'inventaire* qu'il a distribués au sein du sous-compte et retourne un *rapport d'inventaire* au CCIC. Ce rapport contient tous les articles CC 1, CC 2, CC 4, CC 6 et CC 7 de MCC détenus par le sous-compte COMSEC.

13.3.3 Modificatif au rapport d'inventaire

Le *Modificatif au rapport d'inventaire* (GC-223) sert à communiquer tous les écarts entre l'inventaire du sous-compte COMSEC et le *Rapport d'inventaire initial* distribué par le CCIC. Par exemple, si le sous-compte COMSEC a omis de soumettre un *Rapport de destruction* au CCIC, tout le matériel détruit au sous-compte COMSEC qui figurait sur ce *Rapport de destruction* ne sera pas enregistré dans la base de données du CCIC.

Par conséquent, le *Rapport d'inventaire* préparé par le CCIC indiquerait que ce matériel est toujours en stock au sous-compte COMSEC. Le *Modificatif au rapport d'inventaire* fournirait les détails liés au contenu du *Rapport de destruction* manquant.

Lorsqu'il soumet un *Modificatif au rapport d'inventaire*, le gardien de sous-compte COMSEC doit joindre tous les rapports comptables justificatifs pour que le CCIC puisse procéder au rapprochement de l'inventaire.

13.4 Processus d'inventaire

13.4.1 Généralités

Le gardien de sous-compte COMSEC doit faire en sorte qu'un contrôle visuel du stock entier du sous-compte COMSEC soit effectué durant l'inventaire. En prévision du *Rapport d'inventaire périodique* initial distribué par le CCIC, le gardien de sous-compte COMSEC doit s'acquitter des tâches suivantes :

- produire un *Rapport d'inventaire* du sous-compte COMSEC;
- effectuer l'inventaire visuel du MCC remis aux titulaires de prêts ou ordonner à ces derniers de le faire en présence d'un témoin;
- effectuer l'inventaire visuel du matériel COMSEC en stock qui se trouve sous le contrôle direct du gardien de sous-compte COMSEC.

13.4.2 Inventaire visuel

Le gardien de sous-compte COMSEC fournit un *Rapport d'inventaire* aux membres du personnel chargé de réaliser l'inventaire visuel du MCC. Les consignes suivantes s'appliquent au moment de la réalisation d'un inventaire visuel du MCC :

- l'inventaire visuel doit être effectué par deux personnes autorisées qui satisfont aux exigences d'accès au MCC (voir la section 8);
- les deux personnes qui effectuent l'inventaire visuel doivent s'assurer que le MCC en stock correspond au MCC énuméré dans le *Rapport d'inventaire* du sous-compte COMSEC;
- les publications COMSEC non scellées doivent être vérifiées page par page;
- l'équipement cryptographique en cours d'utilisation n'a pas besoin d'être ouvert pour vérifier s'il contient tous les sous-ensembles et éléments requis;
- les ensembles amovibles qui sont énumérés séparément dans le rapport d'inventaire mais qui ne sont pas inscrits sur le boîtier de l'équipement doivent être visuellement contrôlés à moins que l'équipement fasse l'objet de tests ou qu'il soit en cours d'utilisation;
- les clés électroniques stockées dans un équipement comportant une piste de vérification contrôlable peuvent être inventoriées sans la présence d'un témoin.

13.4.3 Rapprochement du rapport d'inventaire de sous-compte COMSEC

13.4.3.1 Rapprochement de l'inventaire des titulaires de prêts

Les personnes chargées de réaliser l'inventaire visant les titulaires de prêts peuvent annoter le *Rapport d'inventaire* pour indiquer que les articles sont en stock ou, inversement, qu'ils ont été perdus, qu'ils sont manquants ou qu'ils existent en nombre excédentaire. Elles doivent toutes les deux signer le *Rapport d'inventaire* avant de le retourner au gardien de sous-compte COMSEC.

Le gardien de sous-compte COMSEC doit rapprocher les *Rapports d'inventaire* retournés par les titulaires de prêts avec le *Rapport d'inventaire* du sous-compte COMSEC.

13.4.3.2 Rapprochement de l'inventaire du sous-compte COMSEC

Le gardien du sous-compte COMSEC doit retourner ses *Rapports d'inventaires* signés au CCIC aux fins de rapprochement. Si des écarts sont relevés dans les rapports du sous-compte COMSEC, le CCIC doit demander au gardien de sous-compte concerné de prendre les mesures correctives appropriées dans les 48 heures, de l'informer des mesures mises en œuvre et de lui envoyer tous les rapports justificatifs nécessaires. Le CCIC doit rapprocher tous les *Rapports d'inventaire*.

13.4.4 Réalisation et soumission des rapports d'inventaire et des documents justificatifs

Après avoir réalisé l'inventaire du sous-compte COMSEC, le gardien de sous-compte COMSEC et le témoin doivent signer et dater le *Rapport d'inventaire*. Le nombre de rapports comptables et de pages de modificatifs doit être indiqué sur la dernière page du *Rapport d'inventaire*.

Le *Rapport d'inventaire*, de même que le *Modificatif au rapport d'inventaire* et les *Rapports de matériel COMSEC* justificatifs (au besoin) doivent être envoyés au CCIC dans les 10 jours ouvrables suivant la réception du *Rapport d'inventaire initial* distribué par le CCIC. Le gardien COMSEC doit conserver un exemplaire signé du *Rapport d'inventaire* dans ses dossiers.

13.4.5 Rapprochement du rapport d'inventaire du sous-compte COMSEC par le CCIC

Le CCIC traite les *rapports d'inventaire* soumis par les sous-comptes COMSEC.

Si le CCIC informe un sous-compte COMSEC qu'il existe des écarts entre son *Rapport d'inventaire* et celui du CCIC, le gardien du sous-compte COMSEC doit tenter de les résoudre.

Si les écarts sont le résultat de *Rapports de matériel COMSEC* manquants, le gardien de sous-compte COMSEC doit préparer et soumettre, dans les 48 heures suivant l'avis lié aux écarts, un *Modificatif au rapport d'inventaire* avec tous les *rapports de matériel COMSEC* justificatifs pour mettre à jour la base de données du CCIC.

Si l'inventaire visuel du sous-compte COMSEC est exact et qu'aucun *Rapport de matériel COMSEC* ne manque, le CCIC produit un *Rapport de rapprochement d'inventaire* attestant l'exactitude de l'inventaire du compte.

Si l'inventaire visuel révèle la perte ou l'absence de MCC ou d'autres écarts, il faut alors signaler un incident COMSEC, tel qu'il est décrit à la section 16. Un *Rapport de rapprochement d'inventaire* n'est produit que lorsque tous les écarts ont été corrigés ou qu'une enquête a été menée sur l'incident et que des consignes ont été données relativement à la disposition.

14 Planification COMSEC en cas d'urgence

14.1 Exigence

Toutes les entreprises du secteur privé qui détiennent du MCC doivent préparer et tenir à jour un *Plan d'urgence COMSEC* consigné pour assurer la protection et le contrôle intégral du MCC. Le *Plan d'urgence COMSEC* doit être utilisé dans les cas suivants :

- les catastrophes naturelles ou les urgences fortuites potentielles (p. ex. ouragans, tornades, tremblements de terre, inondations, incendies); il faut s'efforcer d'incorporer le *Plan d'urgence COMSEC* au *Plan de continuité des activités* établi pour l'ensemble de l'entreprise du secteur privé; les procédures doivent mettre l'accent sur le maintien du contrôle de sécurité sur le MCC jusqu'à ce que l'ordre soit rétabli, sans mettre la vie d'autrui en danger;

- les environnements à risque élevé (p. ex. situations hostiles potentielles ou imminentes); un *Plan d'urgence COMSEC* dans un environnement à risque élevé doit inclure des *Procédures de destruction d'urgence* qui mettent l'accent sur le maintien du contrôle de sécurité sur le MCC jusqu'à ce que l'ordre soit rétabli, sans mettre la vie d'autrui en danger.

14.2 Planification en cas de catastrophes naturelles et d'urgences

La planification doit permettre la réalisation des objectifs suivants :

- la sécurité de tout le personnel;
- la désignation d'un responsable sur place afin d'assurer la protection et le contrôle intégral de tout le MCC;
- la protection ou le retrait du MCC lorsqu'il devient nécessaire d'admettre des personnes non autorisées dans une aire de sécurité;
- l'évacuation des aires;
- l'évaluation des risques d'exposition du MCC à des personnes non autorisées durant la situation d'urgence, et le compte rendu des résultats de cette évaluation;
- l'inventaire du MCC après la situation d'urgence et le signalement à l'ASE, au CCIC et à l'ACM du CCIC de toute perte subie ou de toute exposition non autorisée du MCC;
- l'établissement de sites de reprise principal et secondaire lorsque la reprise est impossible à l'emplacement actuel;
- l'établissement des ressources essentielles nécessaires au soutien de la reprise;
- les installations d'entreposage hors site;
- la continuité des activités durant la situation d'urgence et la reprise subséquente des activités.

14.3 Plan d'urgence

14.3.1 Élaboration

De concert avec le gardien de sous-compte COMSEC, l'ASE est responsable de la préparation, de la mise en œuvre et de la réévaluation annuelle du *Plan d'urgence COMSEC*. La coordination avec le personnel compétent de la sécurité, de la sécurité-incendie et de la sûreté permet d'élaborer un plan réaliste et viable qui favorise l'atteinte des objectifs fixés. Les tâches prévues dans le plan doivent être décrites clairement, et les coordonnées de toutes les personnes chargées d'exécuter des tâches dans le cadre du plan doivent être consignées. Prière de consulter le *modèle de Plan d'urgence COMSEC* pour un aperçu du *Plan d'urgence COMSEC* et des priorités relatives à la destruction d'urgence.

14.3.2 Mise à jour et mise à l'essai du plan

Le gardien de sous-compte COMSEC doit veiller à la réalisation de ce qui suit :

- toutes les personnes responsables de la protection et du contrôle du MCC connaissent l'existence du plan et savent comment les alertes et avertissements liés à une urgence seront communiqués;
- toute personne devant exécuter des tâches dans le cadre du plan reçoit des instructions détaillées sur la façon de les exécuter une fois que le plan est déclenché;

- toutes les personnes connaissent l'ensemble des tâches, de façon à ce que les attributions puissent être modifiées au besoin;
- des exercices périodiques sont effectués pour s'assurer que tous les membres du personnel (surtout les nouveaux) sont en mesure d'accomplir leurs tâches;
- le plan est révisé (au besoin) en fonction de l'expérience acquise lors des exercices.

14.4 Planification des mesures d'urgence

14.4.1 Sous-compte COMSEC évoluant dans des conditions normales

Le gardien de sous-compte COMSEC doit organiser les activités courantes d'exploitation de manière à réduire autant que possible le nombre et la complexité des mesures à adopter en cas d'urgence. Le gardien de sous-compte COMSEC doit veiller à la réalisation de ce qui suit :

- le compte COMSEC détient en tout temps la quantité minimale du MCC requis pour répondre aux besoins opérationnels et d'urgence (voir le Tableau 5);
- le MCC est entreposé de façon à en faciliter, s'il y a lieu, l'évacuation ou la destruction d'urgence;
- la destruction courante est toujours effectuée rapidement dès la réception de l'autorisation;
- le MCC excédentaire est éliminé dans les plus brefs délais, conformément aux instructions pertinentes.

15 Vérification des sous-comptes COMSEC

15.1 Planification de la vérification

15.1.1 Objet de la vérification

La vérification COMSEC offre un processus d'examen indépendant des dossiers et des activités d'un sous-compte COMSEC pour veiller à ce que le MCC produit par le sous-compte, ou confié à celui-ci, soit contrôlé, tel qu'il est détaillé dans la présente directive.

15.1.2 Fréquence des vérifications

Un (ou deux) représentant ou vérificateur désigné par le CCIC vérifiera normalement chaque sous-compte COMSEC au moins tous les 18 mois (voir l'ITSD-08 pour la fréquence des vérifications du MCC en cours de réalisation). Les vérifications peuvent être effectuées plus fréquemment selon un ou plusieurs des facteurs suivants :

- les constats découlant de la vérification précédente;
- la taille de l'inventaire du sous-compte COMSEC;
- le volume des rapports de matériel COMSEC;
- la fréquence des dérogations aux directives COMSEC;
- le nombre anormal de changements de gardien de sous-compte COMSEC;
- le type de système comptable automatisé utilisé au sous-compte COMSEC.

15.1.3 Planification de la vérification

En général, le CCIC donne un préavis de trois semaines avant de procéder à une vérification. Cependant, ledit préavis peut être beaucoup plus court lorsque des irrégularités graves se sont produites. Le cas échéant, le représentant ou le vérificateur que le CCIC aura désigné pour mener la vérification se chargera des tâches suivantes :

- communiquer avec le gardien du sous-compte COMSEC (généralement par téléphone ou par courriel) pour fixer la date de la vérification;
- confirmer par écrit la date et l'heure de la vérification;
- fournir une liste de contrôle servant de guide durant la vérification.

15.2 Réalisation de la vérification

15.2.1 Accès au matériel détenu par le sous-compte COMSEC

Sur présentation de son laissez-passer du CST et d'un exemplaire de son *Attestation d'initiation COMSEC*, le représentant ou le vérificateur désigné par le CCIC est autorisé à accéder sous supervision aux dossiers, aux rapports et aux fichiers du sous-compte COMSEC, y compris les fichiers électroniques et les bases de données.

NOTA 1 : Le représentant du CCIC n'a pas besoin d'autorisation de visite COMSEC, toutefois, le CCIC fournira de l'information sur le visiteur, tel qu'il est énoncé en détail à la section 8.5.

NOTA 2 : Le représentant du CCIC peut demander l'accès supervisé aux emplacements des titulaires de prêts. La vérification des titulaires de prêts doit être coordonnée par le gardien du sous-compte COMSEC.

15.2.2 Portée de la vérification

La portée de la vérification d'un sous-compte COMSEC devrait permettre de déterminer si les enregistrements du sous-compte COMSEC sont exacts et si les procédures de contrôle du MCC ont été suivies correctement et continuent de l'être. La vérification comprend ce qui suit :

- une vérification de l'exactitude et de la complétude des dossiers, des rapports et des fichiers comptables;
- une vérification de la conformité aux procédures d'emballage, de marquage et de distribution;
- une vérification de l'application continue des procédures et des processus (y compris la sécurité physique) relatifs au contrôle, à l'entreposage et à l'utilisation du MCC;
- une évaluation de la pertinence des contrôles du système comptable automatisé;
- un contrôle détaillé des registres comptables du matériel IP, le cas échéant;
- une vérification de la réalisation des vérifications des titulaires de prêts, le cas échéant;
- un entretien avec le gardien de sous-compte COMSEC pour discuter des problèmes rencontrés par ce dernier dans le cadre du contrôle du MCC ou de la tenue du sous-compte COMSEC.

15.2.3 Entrevue de fin de mission

Au terme de la vérification des sous-comptes COMSEC, le représentant du CCIC mènera une entrevue de fin de mission avec l'ASE et le gardien de sous-compte COMSEC pour les informer des situations qui pourraient nécessiter des mesures correctives immédiates et leur faire part des constats et des recommandations découlant de la vérification.

NOTA : L'ASE et le gardien de sous-compte COMSEC doivent tous deux être présents lors de l'entrevue de fin de mission. S'ils ne sont pas disponibles en même temps, le représentant du CCIC doit reporter l'entrevue de fin de mission.

15.3 Rapports de vérification

15.3.1 Rapport de vérification de sous-compte COMSEC

Le *Rapport de vérification* de sous-compte COMSEC consigne toutes les observations et recommandations, de même que toutes les mesures correctives à prendre. Le CCIC transmet à l'ASE un exemplaire du *Rapport de vérification* de sous-compte COMSEC dans les 15 jours ouvrables suivant la date de la vérification. Si des mesures correctives sont nécessaires, un formulaire d'*Attestation des mesures prises* est joint au *Rapport de vérification* de sous-compte COMSEC.

15.3.2 Formulaire Attestation des mesures prises

Le gardien de sous-compte COMSEC doit appliquer les mesures correctives énoncées dans le *Rapport de vérification* de sous-compte COMSEC, puis signer et retourner au CCIC l'*Attestation des mesures prises* dans les 10 jours ouvrables suivant la réception du *Rapport de vérification* de sous-compte COMSEC. Le CCIC peut accorder une prolongation de cette période si, pour des besoins opérationnels, le gardien de sous-compte COMSEC n'est pas en mesure de prendre les mesures requises dans le délai prévu.

15.3.3 Omission de retourner l'Attestation des mesures prises

Le CCIC envoie un avis de recherche à l'ASE s'il ne reçoit pas l'*Attestation des mesures prises* signée dans les délais prescrits. Lorsque l'*Attestation des mesures prises* signée n'est pas reçue au CCIC dans les 10 jours ouvrables suivant l'avis de recherche initial, le CCIC envoie un deuxième avis de recherche à l'ACM du CCIC et met l'ASE ainsi que le gardien de sous-compte COMSEC en copie. Si le CCIC ne reçoit toujours pas l'*Attestation* signée dans les cinq jours ouvrables suivant le deuxième avis de recherche, la situation est traitée comme **un incident COMSEC** et transmise au Bureau national des incidents COMSEC (BNIC) pour que les mesures appropriées soient prises.

16 Incidents COMSEC

16.1 Généralités

Un incident COMSEC se produit lorsqu'une situation ou activité compromet la confidentialité, l'intégrité ou la disponibilité de l'information, du matériel ou des services COMSEC.

Le signalement rapide et exact des incidents COMSEC (p. ex. titulaire de prêts – gardien de sous-compte COMSEC – ASE – CCIC – ACM du CCIC – BNIC) permet de réduire au minimum la possibilité de compromission d'un MCC et de l'information classifiée qu'il protège. Pour que les mesures correctives appropriées soient mises en œuvre prises dans des délais opportuns, il faut absolument que les membres du personnel qui manutentionnent ou gèrent du MCC signalent immédiatement toutes les occurrences d'incidents avérés ou présumés.

En l'occurrence, toute preuve d'incident COMSEC doit être signalée immédiatement au CCIC.

Les rapports sur les incidents COMSEC liés au MCC incluent les incidents liés à la gestion du matériel COMSEC IP (voir l'ITSD-08).

La section 16.8 fournit des exemples d'incidents COMSEC courants.

16.2 Traitement des incidents

16.2.1 Procédure d'identification et d'intervention

L'ASE doit déterminer les procédures internes d'identification des incidents COMSEC et d'intervention, qui assureront le signalement rapide et exact des incidents COMSEC et qui réduiront au minimum la perte ou la compromission réelle ou potentielle d'un MCC.

Le gardien de sous-compte COMSEC doit faire en sorte que chaque personne qui utilise du MCC ou qui y a accès soit en mesure de reconnaître un incident COMSEC et de se conformer à l'exigence de signalement immédiat.

16.2.2 Responsabilité du gardien de sous-compte COMSEC

Lorsqu'un MCC est effectivement ou présumément compromis, le gardien de sous-compte COMSEC doit prendre les mesures suivantes :

1. communiquer immédiatement les circonstances à l'ASE pour que celui-ci signale ensuite l'incident au CCIC;
2. inscrire la mention « enquête en cours » (*Pending Investigation*) sur tout article de MCC touché dans le dossier d'inventaire du matériel COMSEC;
3. continuer de comptabiliser le MCC jusqu'à ce que l'enquête COMSEC soit terminée et qu'un *rapport d'évaluation finale et de clôture* ait été reçu du CCIC, autorisant la disposition du MCC (p. ex. transfert au CCIC aux fins d'évaluation, de destruction et de dispense de comptabilité pour l'article perdu).

16.3 Rapport initial d'incident COMSEC

Le *Rapport initial d'incident COMSEC* sert à signaler les incidents COMSEC et peut être présenté au CCIC par téléphone ou télécopieur sécurisé (voir la section 1.12). Si aucun téléphone ou télécopieur sécurisé n'est disponible, il faut s'entendre avec le CCIC pour livrer le rapport en utilisant le moyen le plus rapide possible. Pour éclaircir certains détails, le CCIC peut également demander un rapport écrit officiel.

Lorsqu'il reçoit le *Rapport initial d'incident COMSEC*, le CCIC évalue la classification de sécurité des prochains rapports et des renseignements supplémentaires, ainsi que les exigences en matière de production de rapports relatives aux obligations du BNIC et de l'ECMCC.

16.4 Rapport d'évaluation d'incident COMSEC

Le *Rapport d'évaluation d'incident COMSEC* (voir l'ITSD-05) fournit des détails sur un incident COMSEC et aide à finaliser l'évaluation des répercussions et les exigences en matière de reprise.

Une fois que le *Rapport initial d'incident COMSEC* du CCIC a été examiné, le CCIC demande, sauf dans des cas très mineurs, un *Rapport d'évaluation d'incident COMSEC*. La demande fait valoir l'importance de fournir les éléments suivants :

- un compte rendu chronologique détaillé de la nature et des circonstances de l'incident;
- de plus amples détails sur l'information contenue dans le *Rapport initial d'incident COMSEC*;
- une description des mesures correctives adoptées pour limiter les dommages causés par l'incident et pour empêcher qu'un incident semblable se reproduise.

16.5 Rapport détaillé

Un rapport détaillé doit être présenté à la demande du CCIC ou dans les cas où l'on découvre des renseignements nouveaux pouvant influencer ou changer le contenu d'un *rapport d'évaluation d'incident COMSEC* précédent.

16.6 Rapport d'évaluation finale et de clôture

Après avoir recueilli et évalué toute l'information disponible à partir des dossiers existants, le BNIC publie un *Rapport d'évaluation finale et de clôture* à l'ACM du CCIC. Le CCIC finalise ensuite l'incident COMSEC avec l'ASE de l'entreprise du secteur privé. Le rapport final fournit des directives sur la façon de prévenir toute récurrence d'incidence similaire ou d'en réduire la possibilité. Il inclut également des instructions sur la disposition du MCC concerné. Le CCIC vérifiera si les recommandations du rapport ont été mises en œuvre.

16.7 Classification et diffusion des rapports

16.7.1 Classification

Un *Rapport d'incident COMSEC* doit être protégé, traité et signalé en fonction du niveau de classification correspondant à celui du MCC exposé, perdu ou compromis, mais jamais à un niveau inférieur au niveau PROTÉGÉ B. Les règles supplémentaires suivantes s'appliquent :

- s'il le juge nécessaire, l'ASE peut classifier un *Rapport d'incident COMSEC* à un niveau supérieur à celui du matériel compromis;
- un *Rapport initial d'incident COMSEC* qui concerne du MCC de niveaux de sensibilité différents doit être protégé, traité et signalé en fonction du niveau de sensibilité le plus élevé applicable à l'incident;
- lorsque le MCC concerné se rapporte à des systèmes TI servant à traiter de l'information à un niveau de classification supérieur à celui du MCC lui-même, l'incident doit être traité et signalé en fonction du niveau de classification le plus élevé (p. ex. un incident lié à une clé d'authentification PROTÉGÉ A qui est utilisée sur un système TI traitant de l'information SECRET sera protégé et signalé au niveau SECRET).

16.7.2 Diffusion

L'information ou les rapports relatifs à un incident COMSEC doivent être communiqués uniquement aux personnes qui ont clairement un besoin de connaître et dont l'habilitation de sécurité correspond au niveau de classification de l'information fournie. Bien que l'information recueillie par le CCIC soit traitée comme de l'information commerciale confidentielle (contenant des renseignements personnels protégés conformément à la *Loi sur la protection des renseignements personnels*), le CCIC peut être tenu de transmettre certains renseignements au ministère parrain du GC, à SPAC ou à d'autres, conformément au PMC ou à l'ITAR.

16.8 Exemples d'incidents COMSEC

Bien qu'elle ne soit pas exhaustive, la liste suivante présente des exemples d'incidents COMSEC qui doivent être signalés au CCIC :

- utilisation prématurée ou hors séquence de clés sans l'approbation de l'AC du réseau cryptographique;
- destruction accidentelle de clés (sans autorisation);
- retrait d'une clé du conditionnement protecteur du fabricant avant sa remise aux fins d'utilisation ou retrait du conditionnement protecteur sans autorisation;
- omission de mettre à zéro un dispositif commun de remplissage (CFD pour *Common Fill Device*) ou un T3MD dans les délais imposés (prière de consulter la doctrine de l'équipement concerné ou de communiquer avec le CCIC pour obtenir des conseils);
- destruction de MCC effectuée en dehors des délais imposés;
- omission de téléverser les données des pistes de vérification des T3MD;
- utilisation d'une clé compromise, remplacée, défectueuse, déjà utilisée (dont la réutilisation n'a pas été autorisée) ou mal utilisée, par exemple :
  - utilisation non autorisée d'une clé à une autre fin que celle prévue,
  - prolongation non autorisée d'une cryptopériode (voir l'ITSD-04),
  - utilisation non autorisée d'un MCC,
  - utilisation prématurée d'une clé;
- application de pratiques opérationnelles ou de maintenance non approuvées par le CST sur des systèmes, de l'équipement et des logiciels cryptographiques approuvés par le CST, par exemple :
  - maintenance d'équipement cryptographique par des personnes non autorisées ou non qualifiées,
  - modification non autorisée ou trafiquage d'un composant, d'un équipement ou d'un système cryptographique;
- utilisation opérationnelle d'un équipement cryptographique dont les circuits de logique cryptographique sont défectueux, ou utilisation d'une procédure d'exploitation non approuvée;
- discussion, par des moyens de communication non sécurisés, portant sur les détails d'une panne ou du fonctionnement défectueux d'un équipement cryptographique;
- utilisation non autorisée d'une clé ou d'un équipement cryptographique approuvé par le CST;
- manquement aux contrôles TPI ou NLZ pour des clés TRÈS SECRET;
- réception d'un équipement classifié, d'un CCI ou d'une clé portant la mention CRYPTO dans un colis dont l'emballage intérieur a été endommagé;
- destruction d'un MCC par des moyens non autorisés;
- maintenance ou tentative de maintenance non autorisée d'équipement cryptographique (y compris la maintenance par des personnes non qualifiées) ou utilisation d'une procédure de maintenance qui s'écarte des directives établies;

- trafiquage présumé ou avéré, pénétration d'un MCC, par exemple, le MCC reçu dans un conditionnement protecteur montrant des signes de trafiquage et d'ouverture prématurée non autorisée;
- copie, reproduction ou photographie non autorisée d'un MCC;
- perte d'un MCC;
- découverte d'un MCC échappant aux contrôles comptables ou physiques requis, notamment :
  - MCC dont la destruction a été consignée dans un rapport de destruction signé par un témoin, mais qui a été découvert non complètement détruit,
  - MCC non sécurisé laissé sans surveillance à un endroit auquel des personnes non autorisées pouvaient avoir accès;
- emballage ou envoi inadéquat d'un MCC.

17 Références

17.1 Liste d'acronymes, d'abréviations et de sigles

AAT	Accord d'assistance technique
AC	Autorité de contrôle
ACM	Autorité COMSEC du ministère
ADR	Autorisation de détenir des renseignements
AND	Agence nationale de distribution
ASE	Agent de sécurité de l'entreprise
ASI	Attestation de sécurité d'installation
ASM	Agent de sécurité du ministère
ASO	Agent de sécurité de l'OSI
BGP	Bureau de gestion du projet
BNIC	Bureau national des incidents COMSEC
CA STI	Chef adjoint, Sécurité des technologies de l'information
CAMC	Centre d'assistance en matière de matériel cryptographique
CC	Code de comptabilité
CCD	Doctrine canadienne en matière de cryptographie (*Canadian Cryptographic Doctrine*)
CCI	Article cryptographique contrôlé (*Controlled Cryptographic Item*)
CCIC	Compte COMSEC industriel du CST
CFD	Dispositif commun de remplissage (*Common Fill Device*)
CFSTI	Centre de formation en sécurité des technologies de l'information
CI	Circuit intégré
CIK	Clé de contact cryptographique (*Cryptographic Ignition Key*)
CKL	Liste des clés compromises (*Compromised Key List*)
COMSEC	Sécurité des communications (*Communications Security*)
ConAuth	Autorité de contrôle (*Controlling Authority*)
CONOP	Concept d'opération
Cryptonet	Réseau cryptographique (*Cryptographic Network*)
CST	Centre de la sécurité des télécommunications
CSTC	Centre de la sécurité des télécommunications Canada
DAAEC	Demande d'autorisation pour l'achat d'équipement COMSEC
DEC	Demande d'équipement COMSEC
DGSM	*Directive sur la gestion de la sécurité ministérielle*
DoS	*Department of State*
DP	Demande de propositions
DSIC	Direction de la sécurité industrielle canadienne
DSII	Direction de la sécurité industrielle internationale
É.-U.	États-Unis
ECMCC	Entente de contrôle du matériel COMSEC comptable
EFG	Équipement fourni par le gouvernement

EKMS GC	Système de gestion électronique des clés du gouvernement du Canada (*Government of Canada Electronic Key Management System*)
EMR	Évaluation des menaces et des risques
GC	Gouvernement du Canada
GRC	Gendarmerie royale du Canada
GSTI	*Gestion de la sécurité des technologies de l'information*
HI/DR	Fiche d'instruction de traitement/fiche d'élimination (*Handling Instructions/Disposition Record*)
ICC	Installation centrale canadienne
ID	Identifiant
IMPC	Inspection des mesures de protection COMSEC
IP	En cours de réalisation (*In-Process*)
ISP	Instruction de sécurité des projets
ITAR	*International Traffic in Arms Regulations*
ITSA	Alerte en matière de sécurité des technologies de l'information (*Information Technology Security Alert*)
ITSB	Bulletin en matière de sécurité des technologies de l'information (*Information Technology Security Bulletin*)
ITSD	Directive en matière de sécurité des technologies de l'information (*Information Technology Security Directive*)
KEK	Clé de chiffrement de clés (*Key Encryption Key*)
KMID	Identificateur de matériel de chiffrement (*Key Material IDentifier*)
KP	Processeur de clés (*Key Processor*)
KSD	Dispositif de stockage de clés (*Key Storage Device*)
KSO	Cadre supérieur clé (*Key Senior Official*)
LE	Lettre d'entente
LGFP	*Loi sur la gestion des finances publiques*
LVERS	Liste de vérification des exigences relatives à la sécurité
MCC	Matériel COMSEC comptable
MCMCI	Manuel de contrôle du matériel COMSEC industriel
MSI	*Manuel de la sécurité industrielle*
NCOR	Bureau national des dossiers (*National Central Office of Record*)
NIP	Numéro d'identification personnel
NLZ	Zone « jamais seul » (*No-Lone Zone*)
ORR	Rapport de remise à la clé opérationnelle (*Operational Rekey Report*)
OTAN	Organisation du Traité de l'Atlantique Nord
PA	Protocole d'accord
PCIE	Propriété, contrôle et influence de l'étranger
PDG	Président-directeur général
PE	Protocole d'entente
PMC	Programme des marchandises contrôlées
PROM	Mémoire morte programmable (*Programmable Read-Only Memory*)

PSG	*Politique sur la sécurité du gouvernement*
PSI	Programme de sécurité industrielle
PSMC	Plan de soutien lié au matériel de chiffrement
PWA	Carte équipée logique (*Printed Wiring Assembly*)
R et E	Réparation et entretien
R.-U.	Royaume-Uni
RMC	*Règlement sur les marchandises contrôlées*
RNEC	Réserve nationale d'équipement cryptographique
RTPC	Réseau téléphonique public commuté
SCIP	Protocole d'interopérabilité des communications sécurisées (*Secure Communications Interoperability Protocol*)
SCC	Services à la clientèle en matière de COMSEC
SCT	Secrétariat du Conseil du Trésor du Canada
SDNS	*Secure Data Network System*
SKCR	Rapport de conversion des clés de diversification (*Seed Key Conversion Report*)
SNCMC	Système national de contrôle du matériel COMSEC
SOA	Attestation des mesures prises (*Statement of Action*)
SPAC	Services publics et Approvisionnement Canada
SPIRS	Sous-système de remise à la clé du RTPC-RNIS du SDNS (*SNDS PSTN-ISDN Rekey Subsystem*)
SSA	Support de stockage amovible
SSI	Secteur de la sécurité industrielle
T3MD	Dispositif de gestion de palier 3 (*Tier 3 Management Device*)
TEK	Clé de chiffrement du trafic (*Traffic Encryption Key*)
TI	Technologies de l'information
TPI	Intégrité par deux personnes (*Two-person Integrity*)
U/FOUO	*UNCLASSIFIED/For Official Use Only*
ULC	Laboratoires des assureurs du Canada (*Underwriters Laboratories of Canada*)
USML	*United States Munitions List*

17.2 Glossaire

Le présent glossaire contient la définition de certains termes qui ont trait au matériel COMSEC faisant l'objet de la présente directive.

Agent de sécurité de l'entreprise (ASE)	Personne-ressource officielle d'une entreprise du secteur privé auprès du Programme de sécurité industrielle responsable de surveiller le profil de sécurité de l'entreprise et de régler les problèmes de sécurité, et devant rendre compte de toutes les questions de sécurité industrielle au Programme de sécurité industrielle et au cadre supérieur clé de l'entreprise.

Agent de sécurité du ministère (ASM)	Personne chargée d'élaborer, de mettre en œuvre, de maintenir, de coordonner et de surveiller un programme de sécurité du ministère conforme à la *Politique sur la sécurité du gouvernement* et aux normes qui s'y rattachent.
Article cryptographique contrôlé (CCI)	Système sécurisé d'information ou de télécommunications, ou composant cryptographique connexe, NON CLASSIFIÉ, mais régi par un ensemble spécial d'exigences en matière de contrôle au sein du Système national de contrôle du matériel COMSEC et portant la mention « article cryptographique contrôlé » (ou « CCI » lorsque l'espace est limité).
Autorité COMSEC du ministère (ACM)	Personne désignée par l'agent de sécurité du ministère et responsable, devant celui-ci, d'élaborer, de mettre en œuvre, de maintenir, de coordonner et de surveiller un programme de sécurité des communications du ministère qui soit conforme à la *Politique sur la sécurité du gouvernement* et aux normes qui s'y rattachent.
Autorité de contrôle (AC)	Entité désignée pour gérer l'utilisation et le contrôle opérationnels d'une clé attribuée à un réseau cryptographique.
Bureau national des incidents COMSEC (BNIC)	Entité du Centre de la sécurité des télécommunications chargée de gérer les incidents liés à la sécurité des communications par l'enregistrement, la validation, l'évaluation et la fermeture des dossiers.
Clé cryptographique	Valeur numérique servant au contrôle des opérations de cryptographie, notamment le déchiffrement, le chiffrement, la génération de signatures ou la validation de signatures.
Clé de contact cryptographique (CIK)	Clé électronique ou dispositif qui peut être utilisé pour accéder au mode sécurisé d'un équipement cryptographique.
Code de comptabilité (CC)	Code numérique servant à indiquer les contrôles de comptabilité minimaux auxquels sont assujettis les articles de matériel COMSEC au sein du Système national de contrôle du matériel COMSEC.
Code de comptabilité 1 (CC 1)	Code numérique attribué au matériel COMSEC comptable électronique et physique faisant l'objet d'une comptabilité continue de la part du Bureau national des dossiers ou d'un bureau central des dossiers, en fonction d'un numéro de série ou d'un numéro de registre, au sein du Système national de contrôle du matériel COMSEC.

Code de comptabilité 2 (CC 2)	Code numérique attribué au matériel COMSEC comptable physique faisant l'objet d'une comptabilité continue de la part du Bureau national des dossiers ou d'un bureau central des dossiers, en fonction de la quantité, au sein du Système national de contrôle du matériel COMSEC.
Code de comptabilité 4 (CC 4)	Code numérique attribué au matériel COMSEC comptable physique ainsi qu'aux clés traditionnelles en format électronique qui, après réception initiale, font l'objet d'une comptabilité locale, en fonction d'un numéro de série ou d'un numéro de registre, au compte COMSEC responsable, au sein du Système national de contrôle du matériel COMSEC.
Code de comptabilité 6 (CC 6)	Code numérique attribué à une clé électronique faisant l'objet d'une comptabilité continue de la part du Bureau national des dossiers ou d'un bureau central des dossiers, en fonction d'un numéro de registre, au sein du Système national de contrôle du matériel COMSEC.
Code de comptabilité 7 (CC 7)	Code numérique attribué aux clés électroniques qui, après réception initiale, font l'objet d'une comptabilité locale (en fonction d'un numéro de registre) au compte COMSEC destinataire préalablement inscrit dans le Système national de contrôle du matériel COMSEC.
Compromission	Accès, divulgation, destruction, suppression, modification, utilisation ou interruption non autorisé de biens ou de renseignements.
Comptabilité	Obligation d'une personne de protéger et de contrôler le matériel COMSEC qui lui a été confié.
Comptabilité locale	Processus par lequel un gardien COMSEC enregistre et contrôle, selon le Système national de contrôle du matériel COMSEC, le matériel COMSEC qu'il n'est pas requis de signaler au Bureau national des dossiers ou à un bureau central des dossiers.
Compte COMSEC industriel du CST (CCIC)	Entité du Centre de la sécurité des télécommunications chargée d'élaborer, de mettre en œuvre, de maintenir, de coordonner et de surveiller le programme de sécurité des communications d'une entreprise du secteur privé et d'en assurer la conformité à la *Politique sur la sécurité du gouvernement* et aux instruments de politique connexes aux fins de gestion du matériel COMSEC comptable.
Conditionnement protecteur	Technique d'emballage du matériel COMSEC qui décourage les pénétrations éventuelles et révèle les pénétrations réelles, ou qui empêche la visualisation ou la copie du matériel COMSEC avant le moment où il sera exposé aux fins d'utilisation.

CRYPTO	Mention, appliquée à une clé ou à un autre matériel COMSEC comptable, qui indique que les articles ainsi marqués sont assujettis à des contrôles particuliers d'accès, de distribution, d'entreposage, de comptabilité, de disposition et de destruction (voir le terme « Cryptographique »).
Cryptographique	Relatif à la cryptographie. **NOTA :** Fréquemment remplacé par la forme abrégée « crypto » utilisée comme préfixe (p. ex. « cryptopériode » pour désigner une période cryptographique).
Cryptopériode	Laps de temps précis durant lequel une clé cryptographique est en vigueur.
Dispositifs de gestion de palier 3 (T3MD)	Équipement cryptographique permettant de stocker, de transporter et de transférer (électroniquement et de façon sécurisée) des clés cryptographiques et qui peut être programmé pour appuyer les systèmes de mission modernes.
Entente de contrôle du matériel COMSEC comptable (ECMCC)	Entente ayant force obligatoire conclue entre le Centre de la sécurité des télécommunications et une entité (du gouvernement ou du secteur privé canadien) ne figurant pas aux annexes I, I.1, II, IV et V de la *Loi sur la gestion des finances publiques*, qui autorise l'acquisition, la comptabilisation, le contrôle, la gestion et la disposition définitive du matériel de sécurité des communications.
Équipement cryptographique	Équipement qui exécute les fonctions de chiffrement, de déchiffrement, d'authentification ou de génération de clés.
Gardien de sous-compte COMSEC	Personne désignée par l'autorité COMSEC d'un ministère comme responsable de la réception, de l'entreposage, de la distribution, de la comptabilité, de la disposition et de la destruction de tout le matériel COMSEC porté au sous-compte COMSEC, ainsi que de l'accès à ce matériel.
Incident COMSEC	Tout événement qui met en péril ou pourrait mettre en péril la sécurité de renseignements classifiés ou protégés du gouvernement du Canada pendant leur stockage, leur traitement, leur transmission ou leur réception.
Inventaire visuel	Vérification physique de la présence de chaque article de matériel COMSEC porté à un compte COMSEC ou à un sous-compte COMSEC.

Matériel COMSEC	Article conçu pour sécuriser ou authentifier l'information de télécommunications. Le matériel COMSEC comprend, sans s'y limiter, les clés cryptographiques, l'équipement, les modules, les dispositifs, les documents, le matériel informatique et les micrologiciels ou logiciels qui comportent ou décrivent une logique cryptographique et d'autres articles qui exécutent des fonctions COMSEC.
Matériel COMSEC comptable (MCC)	Matériel COMSEC qui nécessite un contrôle et une comptabilisation au sein du Système national de contrôle du matériel COMSEC conformément à son code de comptabilité; le transfert ou la divulgation du MCC pose un risque de préjudice à la sécurité nationale du Canada.
Matériel COMSEC en cours de réalisation (IP)	Matériel COMSEC en cours de développement, de production, de fabrication ou de réparation (voir le terme « Matériel COMSEC »).
Matériel cryptographique	Tout le matériel, y compris les documents, les dispositifs et l'équipement, qui contient de l'information cryptographique et qui est indispensable au chiffrement, au déchiffrement ou à l'authentification des communications.
Ordre de mission de messager COMSEC	Certificat qui autorise une personne à transporter des renseignements et des biens classifiés ou protégés.
Parrain du gouvernement du Canada (GC)	Ministère du gouvernement du Canada qui a accepté de parrainer une entreprise du secteur privé autorisée à recevoir (aux fins d'utilisation), à fabriquer, à reproduire ou à réparer du matériel COMSEC comptable et à y accéder.
Remise	Processus de distribution du matériel COMSEC d'un compte COMSEC à un sous-compte COMSEC ou à un titulaire de prêts.
Réseau cryptographique	Au moins deux pièces d'équipement connectées l'une à l'autre, qui utilisent une clé cryptographique pour protéger de l'information.
Sceau Plik	Sceau de sécurité élevée antivol et d'inviolabilité apposé à un colis avant son expédition.
Sécurité des communications (COMSEC)	Application de mesures de sécurité cryptographique, de sécurité des transmissions et des émissions, et de sécurité physique, ainsi que de pratiques et de mécanismes de contrôle opérationnels, visant à empêcher tout accès non autorisé à l'information issue de télécommunications et à garantir l'authenticité de ces télécommunications.

Sous-compte COMSEC	Entité administrative désignée par un numéro unique, créée par un compte COMSEC pour aider au contrôle du matériel COMSEC produit par le compte COMSEC ou confié à celui-ci.
Suivi local	Processus par lequel le gardien COMSEC contrôle et surveille le déplacement des articles de matériel liés à la COMSEC en dehors du Système national de contrôle du matériel COMSEC. **NOTA :** Ce processus n'attribue aucun code de comptabilité.
Support de stockage amovible (SSA)	Dispositif portable utilisé pour transporter ou stocker des données (p. ex. disque, carte mémoire, clé USB).
Système national de contrôle du matériel COMSEC (SNCMC)	Système centralisé, comprenant personnel, formation et procédures, qui permet aux ministères du gouvernement du Canada d'exercer un contrôle intégral et d'effectuer un traitement efficace du matériel COMSEC comptable.
Titre abrégé	Combinaison de lettres et de chiffres attribuée à du matériel COMSEC pour en faciliter la manutention, la comptabilité et le contrôle.
Titulaire de prêts	Personne inscrite auprès d'un compte COMSEC ou d'un sous-compte COMSEC, qui est autorisée à recevoir du matériel COMSEC provenant du compte ou du sous-compte en question.
Transfert	Processus de distribution d'un matériel COMSEC d'un compte COMSEC à un autre compte COMSEC.
Utilisateur autorisé	Personne – autre que le gardien, le gardien suppléant ou le titulaire de prêts – appelée à utiliser du matériel COMSEC dans l'exercice des fonctions qui lui ont été confiées.

18 Bibliographie

Les documents suivants ont servi à l'élaboration de la présente directive :

- **Centre de la sécurité des télécommunications**
  - *Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* (ITSD-03A), mars 2014.
  - *Directive sur l'utilisation de l'équipement COMSEC et des clés approuvés par le CSTC dans un réseau de télécommunication* (ITSD-04), novembre 2011.
  - *Directive sur le signalement et l'évaluation des incidents COMSEC touchant le matériel COMSEC comptable* (ITSD-05), avril 2012.
  - *Écrasement et déclassification des supports d'information électroniques* (ITSG-06), juillet 2006.
  - *Manuel sur la commande de clés cryptographiques* (ITSG-13), mai 2006.
  - *Procédures d'évaluation des installations du gouvernement du Canada* (ITSG-12), juin 2005.
- **Gendarmerie royale du Canada**
  - *Guide d'équipement de sécurité* (G1-001), mars 2006.
  - *Guide pour l'établissement des zones de sécurité matérielle* (G1-026).
- **Ministère de la Justice**
  - *Loi sur la gestion des finances publiques* (LGFP), 1985.
  - *Loi sur la protection des renseignements personnels*, 1985 (version à jour en date du 25 novembre 2012).
  - *Règlement sur les marchandises contrôlées*, 20 mai 2013.
- **Secrétariat du Conseil du Trésor du Canada**
  - *Directive sur la gestion de la sécurité ministérielle* (DGSM), juillet 2009.
  - *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* (GSTI), avril 2004.
  - *Norme opérationnelle sur la sécurité matérielle*, 18 février 2013.
  - *Politique sur la sécurité du gouvernement* (PSG), 1er juillet 2009.
- **Services publics et Approvisionnement Canada**
  - Manuel de la sécurité industrielle, octobre 2014.
- **Underwriters Laboratories of Canada (ULC)**
  - *Underwriters Laboratories of Canada (ULC) Standard* (ULC-S306-03).
- **United States Department of State (U.S. DoS)**
  - *International Traffic in Arms Regulations* (ITAR), 1er avril 2012.

Annexe A Rôles et responsabilités liés au sous-compte COMSEC

A.1 Gardien de sous-compte COMSEC

Les responsabilités du gardien de sous-compte COMSEC incluent ce qui suit :

- assurer la protection et le contrôle du MCC porté au sous-compte COMSEC ou détenu par l'entreprise du secteur privé;
- prendre acte de la participation de l'entreprise aux contrats et aux programmes étrangers ou du GC qui requièrent un soutien en matière de MCC, et consigner les informations pertinentes;
- conserver, dans les dossiers du compte, un exemplaire de toutes les LVERS des contrats, le cas échéant, et assurer la conformité aux exigences qui concernent les activités COMSEC;
- assurer la protection et la comptabilité de tout le MCC remis au sous-compte COMSEC de l'entreprise ou produit dans ses installations;
- tenir à jour les registres COMSEC comptables et les documents connexes, comme il est indiqué dans la présente directive;
- effectuer un inventaire COMSEC et présenter un *Rapport d'inventaire* au CCIC – sur demande du CCIC et lors de la nomination d'un nouveau gardien de sous-compte COMSEC;
- éliminer le matériel COMSEC seulement lorsque les responsables le demandent et utiliser les moyens autorisés à cette fin par le CCIC;
- présenter des rapports d'inventaire, de destruction et de possession au moment opportun;
- veiller à insérer rapidement et méticuleusement tous les modificatifs dans les publications COMSEC (voir la section 11);
- s'assurer que les vérifications de pages sont effectuées pour tout le matériel COMSEC qui l'exige;
- connaître en tout temps l'endroit où se trouve chaque article de MCC détenu par l'installation ainsi que les fins auxquelles il est normalement utilisé;
- établir des procédures « internes » de contrôle strict pour chaque article de MCC lorsque le matériel se trouve à l'extérieur des installations d'entreposage sécurisées du gardien de sous-compte COMSEC;
- s'assurer que le MCC approprié est facilement accessible aux personnes autorisées qui en ont besoin pour s'acquitter de leurs tâches;
- signaler immédiatement à l'ASE tous les incidents COMSEC connus ou soupçonnés;
- aider à la préparation du *Plan d'urgence COMSEC* pour la protection du matériel COMSEC;
- vérifier que les conditions préalables d'accès au MCC ont été respectées avant d'accorder l'accès au matériel ou à tout document ou dossier associé au sous-compte COMSEC;
- informer, par écrit, le personnel de la salle de courrier ou du service de réception des livraisons au sujet de l'exigence de livrer, intacts et directement au gardien de sous-compte COMSEC, tous les colis ou enveloppes qui sont adressés à celui-ci ou qui portent la mention « NE PEUT ÊTRE OUVERT QUE PAR LE GARDIEN DE SOUS-COMPTE COMSEC »;

- prendre part à la préparation de la partie du plan de sécurité de l'entreprise qui traite du matériel COMSEC;
- donner une séance d'initiation COMSEC à tout le personnel qui doit accéder au MCC;
- veiller à ce que le MCC remis dans le cadre d'un contrat particulier ne soit pas utilisé aux fins d'un autre contrat, sauf si le Bureau de gestion du projet (BGP) ou le parrain du GC l'autorise – le cas échéant, informer le CCIC de cette disposition spéciale;
- signaler à l'ASE ou au CCIC, s'il y a lieu, tout problème ou toute préoccupation concernant la gestion du MCC;
- s'assurer que les gardiens suppléants maintiennent le niveau requis de connaissance des exigences du sous-compte COMSEC afin d'assurer la gestion appropriée du sous-compte COMSEC en l'absence du gardien;
- s'assurer que tout le personnel de l'entreprise qui traite ou gère le MCC se conforme à la présente directive;
- veiller continuellement à satisfaire aux besoins en MCC des titulaires de prêts et des utilisateurs;
- s'assurer que tout le MCC est retourné au parrain – par l'entremise du CCIC – à la fin d'un contrat ou d'un accord;
- informer le CCIC de tout changement concernant la gestion du sous-compte COMSEC.

A.2 Gardien suppléant de sous-compte COMSEC

Les tâches du gardien suppléant de sous-compte COMSEC comprennent ce qui suit :

- demeurer au fait des activités courantes du sous-compte COMSEC et offrir son soutien, de façon à être prêt à assumer immédiatement et efficacement, s'il y a lieu, les tâches incombant au gardien de sous-compte COMSEC;
- exécuter les tâches du gardien de sous-compte COMSEC durant toute absence temporaire ne dépassant pas 60 jours civils;
- exécuter les tâches du gardien de sous-compte COMSEC jusqu'à la nomination d'un nouveau gardien, advenant le départ permanent ou une absence non autorisée (60 jours civils ou plus) du gardien attitré.

A.3 Titulaire de prêts

Le MCC est fourni exclusivement aux fins d'utilisation dans une entreprise du secteur privé. Le MCC est prêté à un titulaire de prêts pour une période prédéterminée, et le prêt doit être renouvelé tous les six mois. Le titulaire de prêts rend compte au gardien de sous-compte COMSEC de la protection du MCC qui lui est remis. Toutefois, la responsabilité globale de tout le MCC fourni à l'entreprise repose sur le gardien de sous-compte COMSEC. Les exigences minimales suivantes doivent être respectées :

- le titulaire de prêts doit avoir un besoin de connaître valable;
- le titulaire de prêts doit posséder une *Attestation d'initiation COMSEC* à jour à son dossier;
- le titulaire de prêts doit avoir signé un formulaire *Responsabilités du titulaire de prêts*;
- le titulaire de prêts doit signer l'emprunt et le retour du MCC, selon la méthode de l'accusé de réception ou celle du *Registre de contrôle du matériel COMSEC*;

- le titulaire de prêts doit nécessairement être un utilisateur du matériel (le personnel de bureau ou autre qui n'utilise pas le MCC ne doit pas être nommé à titre de titulaire de prêts);
- le titulaire de prêts doit répondre aux exigences d'accès au MCC;
- le titulaire de prêts doit consentir à ce que le MCC dont il est responsable soit l'objet d'inspections sans préavis menées par le personnel de garde du sous-compte COMSEC;
- le MCC détenu par le titulaire de prêts doit faire l'objet d'un contrôle visuel officiel, tel qu'il est détaillé dans la présente directive;
- le titulaire de prêts doit immédiatement informer le personnel de garde de toute infraction ou de tout incident de sécurité COMSEC;
- lorsque de l'équipement cryptographique (classifié ou CCI) est utilisé, le titulaire de prêts doit apprendre à utiliser ledit équipement grâce à une formation prodiguée en milieu de travail par le gardien de sous-compte COMSEC ou grâce à un autre type de formation approuvée par le CST.

Annexe B Procédures de réception du matériel COMSEC comptable

B.1 Préparation en prévision de la réception du matériel COMSEC comptable

Avant de recevoir du MCC, le gardien de sous-compte COMSEC du ministère doit procéder à ce qui suit :

- fournir au personnel de la salle de courrier ou de l'aire de réception de l'entreprise les renseignements suivants :
  - nom du sous-compte COMSEC de l'entreprise qui a été établi;
  - nom et adresse interne du gardien de sous-compte COMSEC;
  - exigence de livrer au gardien de sous-compte COMSEC le courrier et les colis adressés au sous-compte COMSEC, non ouverts;
- demander au personnel de la salle de courrier ou de l'aire de réception de l'entreprise qui aurait ouvert par inadvertance l'emballage extérieur d'un colis, de conserver cet emballage et de le remettre au gardien de sous-compte COMSEC avec le colis;
- fournir à la salle de courrier ou à l'aire de réception de l'entreprise des exemplaires à jour du formulaire *Demande de pouvoir de signature COMSEC*;
- veiller à ce que les personnes autorisées à accuser réception des colis puissent procéder à l'entreposage sécurisé desdits colis (lorsque le gardien de sous-compte COMSEC ou le gardien suppléant est absent).

B.2 Inspection des colis

À la réception d'un envoi, le gardien de sous-compte COMSEC doit procéder comme suit :

- examiner attentivement les emballages extérieur et intérieur avant de les enlever du colis, de façon à relever, s'il y a lieu, tout signe de dommage ou de trafiquage;
- vérifier les adresses sur les emballages extérieur et intérieur pour savoir si le colis a bel et bien été livré au bon destinataire;
- communiquer sur-le-champ toute apparence d'accès non autorisé au contenu ou de trafiquage de l'emballage intérieur ou extérieur comme le signe d'un incident COMSEC potentiel, tel qu'il est expliqué en détail à la section 16 :
  - en attendant l'enquête sur une compromission possible, mettre fin au déballage du colis et placer ce dernier en quarantaine;
  - avertir le gardien de sous-compte COMSEC expéditeur d'ajouter l'état « Enquête en cours » (*Pending Investigation*) à tout le MCC concerné.

B.3 Équipement cryptographique scellé

L'équipement cryptographique livré dans des contenants d'expédition spécialisés et scellés qui n'ont pas été ouverts et qui ne montrent aucun signe de trafiquage peut être accepté sans examen visuel du contenu, à condition que l'étiquette spéciale apposée au contenant soit conforme à ce qui est indiqué sur le *rapport de matériel COMSEC*. Dans le cas contraire, le contenu physique doit être inventorié. Bien qu'il ne soit pas nécessaire d'ouvrir certains types de matériel avant de les utiliser, le gardien de sous-compte COMSEC ne doit pas oublier qu'il doit prévoir suffisamment de temps pour obtenir les pièces de remplacement pour des articles incomplets ou défectueux. De plus, le gardien de sous-compte COMSEC est responsable de signaler au CCIC tout écart noté au moment de la livraison.

Annexe C Acquisition d'équipement cryptographique comptable

C.1 Généralités

A priori, une entreprise du secteur privé canadien n'est pas autorisée à acquérir ni à posséder de l'équipement cryptographique comptable. Toutefois, si elle est parrainée par un ministère du gouvernement du Canada (GC) qui a établi un compte COMSEC, elle pourra disposer d'équipement cryptographique comptable (y compris les clés, l'équipement auxiliaire et les doctrines portant sur l'équipement). Les Services à la clientèle en matière de COMSEC doivent coordonner la signature d'une *Entente de contrôle du matériel COMSEC comptable* (ECMCC) entre toutes les parties (voir la section 1.7).

NOTA : Bien qu'une entreprise du secteur privé ne soit pas autorisée à acquérir du MCC, son parrain du GC peut appliquer un recouvrement des coûts pour l'équipement fourni. L'ECMCC ou une entente officielle doit clairement stipuler que l'équipement (notamment les clés et l'équipement auxiliaire) sera retourné au parrain du GC (par l'entremise du CCIC) aux fins de disposition dès qu'il ne sera plus requis, conformément aux modalités de l'ECMCC ou de l'entente officielle.

Le parrain du GC doit obtenir l'approbation des Services à la clientèle en matière de COMSEC avant de fournir (par l'entremise du CCIC) l'équipement cryptographique comptable à une entreprise du secteur privé. L'approbation sera fondée, entre autres, sur les critères suivants :

- la nature et l'ampleur de la propriété, du contrôle et de l'influence de l'étranger (PCIE), voir la section 1.11.1;
- le type et la classification de l'équipement cryptographique qui sera remis;
- le niveau d'accès requis;
- l'attestation de sécurité d'installation (ASI);
- l'autorisation de détenir des renseignements (ADR);
- l'inspection des mesures de protection COMSEC (IMPC).

C.2 Acquisition en vertu d'un contrat du gouvernement du Canada

L'équipement cryptographique comptable peut être fourni à une entreprise du secteur privé canadien dans le cadre d'un contrat passé avec Services publics et Approvisionnement Canada (SPAC).

Le contrat doit indiquer précisément, dans la Liste de vérification des exigences relatives à la sécurité (LVERS), le besoin de détenir et d'utiliser l'équipement en question (notamment les clés et l'équipement auxiliaire pertinents).

C.3 Acquisition sans contrat du gouvernement du Canada

En temps normal, le MCC peut être fourni à une entreprise du secteur privé sans la conclusion d'un contrat du GC négocié par SPAC, à condition que l'entreprise ait établi un sous-compte COMSEC, tel qu'il est détaillé à la section 5.1.

Dans des circonstances exceptionnelles (p. ex. lors d'événements spéciaux parrainés par le gouvernement), les Services à la clientèle en matière de COMSEC peuvent autoriser un prêt de MCC à court terme (y compris les clés connexes) à une entreprise suivant la conclusion d'un accord de parrainage, et ce, sans avoir à établir un sous-compte COMSEC.

NOTA : Lorsque le MCC (y compris les clés et l'équipement connexe) n'est plus requis pour les activités mentionnées précédemment, il doit être retourné à son propriétaire par l'entremise du CCIC.

C.4 Installation de l'équipement cryptographique comptable

Le ministère parrain du GC est responsable d'effectuer une évaluation des menaces et des risques (EMR) ainsi qu'une évaluation de la sécurité et autorisation avant de permettre à l'entreprise parrainée d'utiliser l'équipement.

C.5 Exigences relatives aux clés

Le ministère parrain du GC est responsable d'établir les privilèges associés à la commande des clés et de commander les clés auprès du CST. Le CCIC est responsable de la livraison et de la gestion des clés.

C.6 Procédure d'acquisition

Les sept étapes énumérées ci-dessous s'appliquent à toute entreprise du secteur privé appelée à détenir de l'équipement cryptographique comptable pour satisfaire aux exigences d'un contrat du GC obtenu par l'entremise de SPAC.

1. L'ASM ou l'ACM du ministère parrain du GC doit définir les besoins de l'entreprise du secteur privé en matière de COMSEC dès le début du processus d'attribution du contrat.
2. Le parrain du GC présentera une demande écrite et détaillée aux Services à la clientèle en matière de COMSEC. Il doit inclure une DEC et une DAAEC dûment remplies, le cas échéant. S'il y a lieu, il fournira de la documentation supplémentaire, par exemple, un concept d'opération (CONOP), un PSMC ou un plan IP. Les besoins relatifs aux autres articles de MCC (p. ex. les clés et les publications) doivent également être établis sans tarder.
3. Advenant qu'au terme de la procédure d'examen et de validation, les Services à la clientèle en matière de COMSEC estiment que les besoins sont justifiés, le CST fait parvenir au parrain du GC une lettre de confirmation (qui inclut simplement un accusé de réception et une attestation de la validité des besoins). L'autorisation finale de la remise est accordée par les Services à la clientèle en matière de COMSEC, une fois que toutes les exigences de sécurité ont été appliquées (voir l'étape 6). À ce stade, le CST produit une ECMCC.
4. Le parrain présente au PSI de SPAC une trousse d'information contenant la lettre de confirmation du CST, une LVERS remplie et signée, de même qu'un exemplaire de l'accord officiel de parrainage (p. ex. contrat, entente préalable au contrat ou autre type d'accord de parrainage). Un exemplaire de la LVERS doit également être transmis aux Services à la clientèle en matière de COMSEC.

   NOTA 1 : L'accord de parrainage doit préciser le nom de l'entreprise et son emplacement, décrire le travail à effectuer, établir les CCI du GC et tout autre MCC nécessaire à l'exécution du contrat, indiquer la méthode d'acquisition de l'équipement de même que la façon dont les CCI et le reste du matériel COMSEC seront utilisés.

   NOTA 2 : Le parrain du GC devrait communiquer avec les Services à la clientèle en matière de COMSEC pour obtenir des conseils sur la façon de remplir la LVERS en vue de satisfaire aux exigences COMSEC. Bien que la LVERS doive décrire l'IMPC en tenant compte du plus haut niveau de sensibilité du MCC utilisé, le niveau minimal doit être SECRET.

5. Lorsque le personnel du PSI de SPAC reçoit la trousse d'information du ministère parrain, il doit procéder à ce qui suit :
   - communiquer avec l'entreprise du secteur privé et confirmer qu'elle satisfait aux exigences de sécurité de l'accord de parrainage ou de la LVERS;
   - une fois le respect des exigences de sécurité confirmé, informer l'entreprise qu'on lui a adjugé le contrat (PCIE, ASI et inspections liées à l'ADR, aux TI et à la production, le cas échéant); le parrain du GC et les Services à la clientèle en matière de COMSEC recevront un exemplaire de la lettre d'adjudication.
6. Lorsque les Services à la clientèle en matière de COMSEC reçoivent l'avis du PSI, ils autorisent l'établissement du sous-compte COMSEC de l'entreprise et s'assurent que toute la documentation connexe, y compris l'ECMCC, est complète et approuvée.

   S'il existe déjà un sous-compte COMSEC du secteur privé dont le niveau de sensibilité est équivalent, les Services à la clientèle en matière de COMSEC prennent les mesures nécessaires pour remplir et approuver l'ECMCC, le PA et le PE requis (le cas échéant). L'autorisation finale du CST concernant la remise du MCC aux partenaires du secteur privé est promulguée par les Services à la clientèle en matière de COMSEC.
7. Lorsque le parrain du GC reçoit l'avis du PSI, il transfère au CCIC l'équipement cryptographique ou autre MCC du GC dans le Système national de contrôle du matériel COMSEC (SNCMC). Une fois que les Services à la clientèle en matière de COMSEC autorisent la remise, le CCIC remet le MCC au sous-compte COMSEC concerné.

   NOTA 1 : Le MCC ne sera pas transféré du CST tant que le CCIC n'aura pas établi le sous-compte COMSEC.

   NOTA 2 : Prière de communiquer avec les Services à la clientèle en matière de COMSEC pour obtenir des conseils sur l'acquisition de MCC pour des motifs autres que la conformité aux exigences d'un contrat du GC obtenu par l'entremise de SPAC (p. ex. les exigences liées aux demandes de propositions [DP] – voir la section 8.1.3).

Annexe D Rôles et responsabilités – Guide de référence

D.1 Rôles et responsabilités – Avec un contrat du gouvernement du Canada

Le tableau suivant sert de guide de référence sur les principaux rôles et responsabilités du Centre de la sécurité des télécommunications (CST), de Services publics et Approvisionnement Canada (SPAC), du parrain du GC et de l'entreprise du secteur privé dans les situations où l'entreprise du secteur privé détient un contrat obtenu par l'entremise de SPAC et en vertu duquel elle doit détenir du matériel COMSEC comptable (MCC).

Tableau 7 – Rôles et responsabilités – Avec un contrat du gouvernement du Canada

SCC = Services à la clientèle en matière de COMSEC	CST		PSI de SPAC	Parrain du GC	Entreprise du secteur privé
	CCIC	SCC			
Informer le CST des dispositions d'un contrat ou d'une entente en vertu desquelles l'entreprise doit accéder au MCC				▲ 2.5	
Signer les *ententes de contrôle du matériel COMSEC comptable* (ECMCC)				▲ 2.5	▲ 2.6.2
S'assurer que les Services à la clientèle en matière de COMSEC ont reçu la LVERS				▲ 2.5	
Fournir des inspections équivalentes à l'attestation de sécurité d'installation (ASI), l'autorisation de détenir des renseignements (ADR) et l'inspection des mesures de protection COMSEC (IMPC), tel que l'exige le CST				▲ 2.5	
Déterminer les besoins en MCC et présenter une DEC et une DAAEC au CST (le cas échéant)				▲ 2.5 et annexe C.6	
Fournir une autorité de contrôle pour les réseaux cryptographiques autorisés				▲ 2.5	
Coordonner la diffusion de MCC à une entreprise du secteur privé avec le CCIC				▲ 2.5	
Effectuer une évaluation PCIE			▲ 1.11.1 et 2.3.1		

SCC = Services à la clientèle en matière de COMSEC	CST		PSI de SPAC	Parrain du GC	Entreprise du secteur privé
	CCIC	SCC			
Fournir une ASI, une ADR et une IMPC			▲ 2.3.1		
Fournir une évaluation de la pertinence d'effectuer une évaluation PCIE ainsi que des inspections liées à l'ASI, à l'IMPC, à l'ADR et à la production			▲ 8.1.3		
Coordonner la vérification de sécurité des entreprises du secteur privé et de leur personnel conformément aux exigences de sécurité des contrats étrangers et de l'Organisation du Traité de l'Atlantique Nord (OTAN)			▲ 2.3.1		
Organiser le transfert de renseignements et de biens non-COMSEC protégés et classifiés entre les gouvernements canadien et étrangers et le secteur privé			▲ 2.3.1		
Coordonner l'élaboration d'instructions sur la sécurité des projets (ISP) internationales			▲ 2.3.1		
Fournir les autorisations de permis de visite			▲ 2.3.1		
Ouvrir et fermer un sous-compte COMSEC	▲ 2.2.3, 5.1 et 5.5				
Autoriser et coordonner le déplacement et la distribution du MCC	▲ 2.2.3				
Fournir du soutien et des conseils relativement à l'utilisation des clés et de l'équipement cryptographiques approuvés par le CST	▲ 2.2.3				
Effectuer les rapprochements d'inventaire annuel	▲ 2.2.3				

SCC = Services à la clientèle en matière de COMSEC	CST		PSI de SPAC	Parrain du GC	Entreprise du secteur privé
	CCIC	SCC			
Agir à titre de personne-ressource initiale du CST pour le signalement des incidents COMSEC	▲ 16.1				
Effectuer la vérification des sous-comptes COMSEC du secteur privé	▲ 2.2.3 et 15.1.2				
Fournir des conseils, des directives et une orientation concernant la gestion COMSEC	▲ 2.2.3				
Suspendre temporairement un sous-compte COMSEC	▲ 5.7				
Autoriser les changements aux codes de comptabilité	▲ 6.2.5.1				
Offrir des séances d'initiation COMSEC au gardien de sous-compte COMSEC	▲ 8.2.1				
Approuver l'aire de travail du gardien de sous-compte COMSEC	▲ 9.2				
Autoriser l'entreposage ou la livraison d'équipement mis à la clé	▲ 9.6.2 et 10.4				
Autoriser la sélection des messagers des entreprises du secteur privé	▲ 10.10.1				
Effectuer la vérification des comptes COMSEC IP	▲ ITSD-08				
Donner des conseils et des directives sur le déplacement de MCC assujettis au contrôle de l'ITAR		▲ 2.2.1			
Fournir une évaluation de la pertinence de détenir un sous-compte COMSEC		▲ 2.2.1 et 8.1.3			
Autoriser l'établissement ou la fermeture d'un sous-compte COMSEC du secteur privé		▲ 2.2.1			

SCC = Services à la clientèle en matière de COMSEC	CST		PSI de SPAC	Parrain du GC	Entreprise du secteur privé
	CCIC	SCC			
Autoriser l'établissement et la fermeture d'un compte COMSEC IP		▲ ITSD-08			
Valider les besoins du secteur privé de détenir des solutions et du matériel COMSEC approuvés par le CST		▲ 2.2.1			
Confirmer le respect de toutes les conditions préalables en matière de sécurité avant d'autoriser l'établissement d'un sous-compte		▲ 2.2.1			
Coordonner la signature et la diffusion des ECMCC, des AAT, des ententes de non-divulgation et d'autres accords		▲ 2.2.1 et annexe C.1			
Valider les plans de soutien lié au matériel de chiffrement		▲ 2.2.1			
Coordonner l'exécution des inspections TEMPEST		▲ 2.2.1			
Coordonner les expéditions transfrontalières de MCC avec les autres autorités responsables de la sécurité nationale		▲ 2.2.1			
Autoriser les accès COMSEC pour les visites		▲ 4.2.1 et 8.5			
Autoriser les changements au niveau de classification d'un sous-compte COMSEC		▲ 5.3.4			
Autoriser un solde nul pour un sous-compte COMSEC		▲ 5.6			
Autoriser des ressortissants étrangers à accéder au MCC		▲ 8.1.2			
Autoriser les aires de travail situées à l'extérieur des installations COMSEC établies		▲ 9.1.1			
Approuver les plans IP		▲ ITSD-08			

SCC = Services à la clientèle en matière de COMSEC	CST		PSI de SPAC	Parrain du GC	Entreprise du secteur privé
	CCIC	SCC			
Mettre en œuvre les exigences du Programme des marchandises contrôlées du Canada et de l'*International Traffic in Arms Regulations* des É.-U.					▲ 1.11.2 et 1.11.3
S'assurer que la gestion du MCC dans l'entreprise répond aux normes minimales exigées par le CST					▲ 2.6.2
Présenter au CCIC un certificat de nomination pour le gardien de sous-compte COMSEC et les gardiens suppléants					▲ 5.1.2
Donner des séances d'initiation COMSEC au personnel de sous-compte COMSEC					▲ 8.2.1
Élaborer un *plan d'urgence COMSEC*					▲ 2.6.2 et 14.3.1
Élaborer un plan IP					▲ ITSD-08
Signaler les incidents COMSEC au CCIC					▲ 2.2.3, 16 et ITSD-05
Veiller à ce que les sous-traitants respectent les exigences de sécurité énoncées dans le MSI de SPAC et dans la présente directive avant de leur permettre l'accès au MCC					▲ 2.6.2

D.2 Rôles et responsabilités – Sans contrat du gouvernement du Canada

Les rôles et responsabilités présentés dans le Tableau 7 concernent toute entreprise du secteur privé qui doit détenir du matériel COMSEC comptable (MCC) sans passer de contrat avec le GC, à l'exception des éléments suivants (exigés par le CST) fournis par le parrain du GC et validés par les Services à la clientèle en matière de COMSEC :

- équivalent d'une ASI (attestation de sécurité d'installation);
- équivalent d'une ADR (autorisation de détenir des renseignements);
- traitement de la technologie de l'information (ITP pour *Information Technology Processing*);
- inspection des mesures de protection COMSEC (IMPC);
- documents connexes supplémentaires.