Conseil canadien des normes
Standards Council of Canada

Exigences relatives à l'accréditation des installations d'essais de modules et d'algorithmes cryptographiques

CAN-P-1621
juin 2004

système national de normes

Canada

EXIGENCES RELATIVES À L'ACCRÉDITATION DES INSTALLATIONS D'ESSAIS DE MODULES ET D'ALGORITHMES CRYPTOGRAPHIQUES

REQUIREMENTS FOR THE ACCREDITATION OF CRYPTOGRAPHIC MODULE AND ALGORITHM TESTING FACILITIES

CAN-P-1621

Juin 2004

Conseil canadien des normes
270, rue Albert, bureau 200
Ottawa (Ontario)
K1P 6N7 Canada
Tél. : (613) 238-3222
Télec : (613) 569-7808
Courriel: info@scc.ca

NOTE : An English version of this document is available from the:

Standards Council of Canada
270 Albert Street, Suite 200
OTTAWA, Ontario
K1P 6N7
Tel.: (613) 238-3222
Fax.: (613) 569-7808
Internet: info@scc.ca

TABLE DES MATIÈRES

AVANT-PROPOS

Le Conseil canadien des normes (« CCN ») est une société d'État constituée en vertu d'une loi adoptée par le Parlement en 1970, qui a été modifiée en 1996, pour encourager au Canada une normalisation volontaire efficiente et efficace. Bien que financé en partie en vertu d'un crédit parlementaire, il est indépendant du gouvernement pour ce qui est de ses politiques et de son fonctionnement. Le Conseil du CCN est composé de personnes issues du gouvernement et d'organisations du secteur privé.

Le CCN a pour mission d'inciter les Canadiens à participer aux activités de normalisation volontaire; d'encourager au Canada la collaboration entre les secteurs privé et public dans le domaine de la normalisation volontaire; de coordonner les efforts des personnes et organisations engagées dans les activités du Système national de normes, de favoriser, dans le cadre des activités relatives à la normalisation, la qualité, la performance et l'innovation technologique liées aux produits et services canadiens; d'élaborer des stratégies de normalisation et de définir des objectifs à long terme en matière de normalisation.

Par essence, le CCN encourage au Canada une normalisation efficiente et efficace, lorsque celle-ci ne fait l'objet d'aucune mesure législative, en vue de faire progresser l'économie nationale, de contribuer au développement durable, d'améliorer la santé, la sécurité et le bien-être des travailleurs et du public, d'aider et de protéger les consommateurs, de faciliter le commerce intérieur et extérieur, et de développer la coopération internationale en matière de normalisation.

En outre, le CCN est le point de convergence du gouvernement dans le domaine de la normalisation volontaire et représente le Canada dans le cadre des activités internationales de normalisation. Il établit les politiques et procédures nécessaires à l'élaboration des Normes nationales du Canada et à l'accréditation des organismes d'élaboration de normes, des organismes de certification de produits, des laboratoires d'essais et d'étalonnages, des organismes registraires des systèmes de gestion de la qualité et de management environnemental, des organismes de certification des auditeurs environnementaux et des prestataires de cours de formation des auditeurs. Enfin, le CCN se fait le défenseur de la reconnaissance des systèmes d'accréditation et autres systèmes équivalents pour réduire le nombre d'évaluations et d'audits, principe qu'il défend dans son pays et avec les partenaires commerciaux de ce dernier.

Le présent document fait partie de ceux qui ont été publiés par le Conseil canadien des normes pour définir les politiques, les projets et les méthodes qu'il a établis pour l'aider à remplir son mandat.

Toute demande d'éclaircissement, toute recommandation proposant des modifications au présent document et toute demande d'exemplaires de ce dernier doivent être adressées à l'éditeur.

PRÉFACE

Le présent document, le CAN-P-1621, présente les exigences particulières du Conseil canadien des normes s'appliquant aux installations d'essais candidates à une accréditation en vue de la conduite d'évaluations de la conformité de modules cryptographiques à la norme FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, mise au point par le National Institute for Standards and Technology du gouvernement des États-Unis et le Centre de la sécurité des télécommunications du gouvernement du Canada.

Le présent document a été préparé pour la gouverne et à l'usage des accréditeurs, du personnel des installations d'essais de modules et d'algorithmes cryptographiques, des installations candidates à l'accréditation, des autres systèmes d'accréditation de laboratoires et des clients d'installations d'essais, ainsi que des organisations ou des personnes qui ont besoin d'information sur les conditions d'accréditation en vertu du programme d'accréditation des installations d'essais de modules et d'algorithmes cryptographiques.

Le CAN-P-1621 fournit des lignes directrices expresses qui complètent celles du document CAN-P-1591B : 2001, *Lignes directrices relatives à l'accréditation des installations d'évaluation et d'essais de produits de sécurité des technologies de l'information.* Les exigences techniques sont expliquées afin d'indiquer comment ces lignes directrices particulières s'appliquent.

Toute installation (y compris celles qui sont exploitées par des entreprises, des fabricants, des universités, ou encore par le gouvernement fédéral ou des gouvernements provinciaux) qui applique des méthodes d'essai, notamment aux modules et aux algorithmes cryptographiques, peut présenter une demande d'accréditation au CCN. Pour obtenir l'accréditation, les installations doivent satisfaire aux exigences énoncées dans le présent document ainsi qu'à celles qui sont précisées dans le Guide du PALCAN, *Programme d'accréditation des laboratoires*. L'accréditation ne fournit pas de garantie concernant la performance des installations ou les résultats des essais; elle établit la compétence d'une installation.

Les termes *laboratoire* et *installation d'essais* sont employés de manière interchangeable tout au long du document et sont considérés comme des synonymes.

INTRODUCTION

a) Programme de validation des modules cryptographiques

Le 17 juillet 1995, le National Institute of Standards and Technology (NIST) du Department of Commerce des États-Unis et le Centre de la sécurité des télécommunications (CST) ont annoncé la création du Programme de validation des modules cryptographiques (PVMC). Le PVMC permet la validation de produits commerciaux en fonction de la norme FIPS 140-2, *Security Requirements for Cryptographic Modules*. Les produits validés en vertu de ce programme peuvent être utilisés au Canada et aux États-Unis pour la protection de renseignements non classifiés de nature délicate.

Le PVMC a besoin d'installations d'essais accréditées et indépendantes pour mettre des produits à l'essai en vue de leur validation en fonction de la norme FIPS 140-2. Le NVLAP (*National Voluntary Laboratory Accreditation Program*) du NIST permet d'accréditer les installations d'essais qui répondent aux exigences contenues dans le guide 150, *NVLAP Procedures and General Requirements*, et le guide 150-17, *Cryptographic Module Testing*, du NIST.

Le CAN-P-1621 précise les exigences liées à l'accréditation, par le Conseil canadien des normes (CCN), des installations d'essais pour l'exécution d'évaluations de la conformité en vertu de la norme FIPS 140-2; les installations accréditées sont reconnues en vertu du PVMC.

b) FIPS 140-2, Security Requirements for Cryptographic Modules

La norme FIPS 140-2 précise les exigences de sécurité auxquelles doit répondre le module de chiffrement d'un système de sécurité protégeant l'information classifiée à l'intérieur de systèmes informatiques et de télécommunications (y compris les systèmes de transmission de la voix). Les exigences de sécurité portent sur la conception et la mise en oeuvre sûres d'un module de chiffrement, et plus particulièrement sur les éléments suivants : conception et documentation de base; interfaces de module; rôles, services autorisés et méthodes authentification; sécurité physique; sécurité logicielle; environnement opérationnel; gestion des clés cryptographiques; interférence et compatibilité électromagnétiques; auto-vérification; et la mitigation de d'autres types d'attaques.

La norme FIPS 140-1 est en vigueur depuis janvier 1994 et a récemment fait l'objet d'une révision (exercice mené tous les cinq ans) par le NIST et le CST, en fonction de la technologie actuelle. La norme révisée portera le titre de FIPS 140-2: *Security Requirements for Cryptographic Modules*.

c) CAN-P-1621, Exigences relatives à l'accréditation des installations d'essais de modules et d'algorithmes cryptographiques

Le CAN-P-1621 précise les exigences propres à l'évaluation de modules et d'algorithmes cryptographiques en vue de déterminer leur conformité à la norme FIPS 140-2. Les exigences génériques liées aux installations d'essais qui sont précisées dans le guide 150 et le guide 150-17 ont été relevées et mises en correspondance avec les exigences précisées dans les guides PALCAN, CAN-P-4D et CAN-P-1591B. Les autres exigences qui s'appliquent aux modules et aux algorithmes cryptographiques ont été regroupées dans le présent document. Par conséquent, la somme des liens établis dans les documents CAN-P-4D, CAN-P-1591B et CAN-P-1621 équivaut à toutes les exigences précisées dans les guides 150 et 150-17. La figure 1 illustre les correspondances établies.

Le présent document vise à définir les exigences additionnelles applicables à l'accréditation des installations d'essais, c'est-à-dire les exigences s'ajoutant à celles déjà formulées dans les documents CAN-P-4D et CAN-P-1591B concernant les aspects techniques et organisationnels, en vue de la conduite d'évaluations de la conformité des modules cryptographiques et des algorithmes correspondants à la FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*.

Le CAN-P-1622, *Liste de contrôle applicable à l'évaluation des installations d'essais de modules et d'algorithmes de chiffrement*, est la liste de contrôle à utiliser pour l'évaluation des installations d'essais en fonction des exigences précisées dans le présent document.

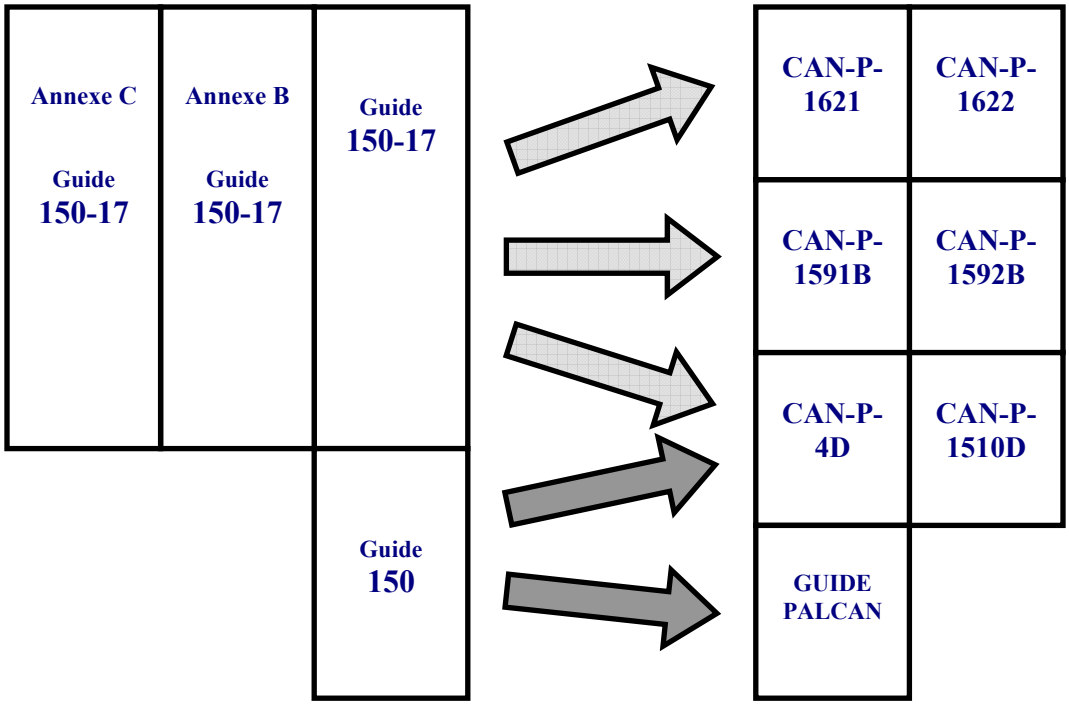

Figure 1 – Établissement des correspondances en matière d'exigences entre les guides du NIST et les documents du CCN

d) Cadre d'accréditation du CCN

Le CCN a élaboré un cadre d'accréditation dans lequel s'inscrit une norme complétant d'autres normes de nature plus générale. Voir la figure 2 ci-dessous. Le PALCAN (non illustré) décrit le processus d'accréditation des installations d'essais. Le CAN-P-4D précise les exigences générales auxquelles doivent répondre toutes les installations d'essais voulant être accréditées. Le CAN-P-1591B se veut un supplément au CAN-P-4D en ce qui a trait aux évaluations et aux essais de produits de sécurité des technologies de l'information (EEPSTI). Le présent document précise en outre les exigences auxquelles doit répondre une installation d'EEPSTI pour évaluer des modules et des algorithmes cryptographiques. Le cadre proposé permet l'ajout d'autres secteurs d'essais spécialisés.

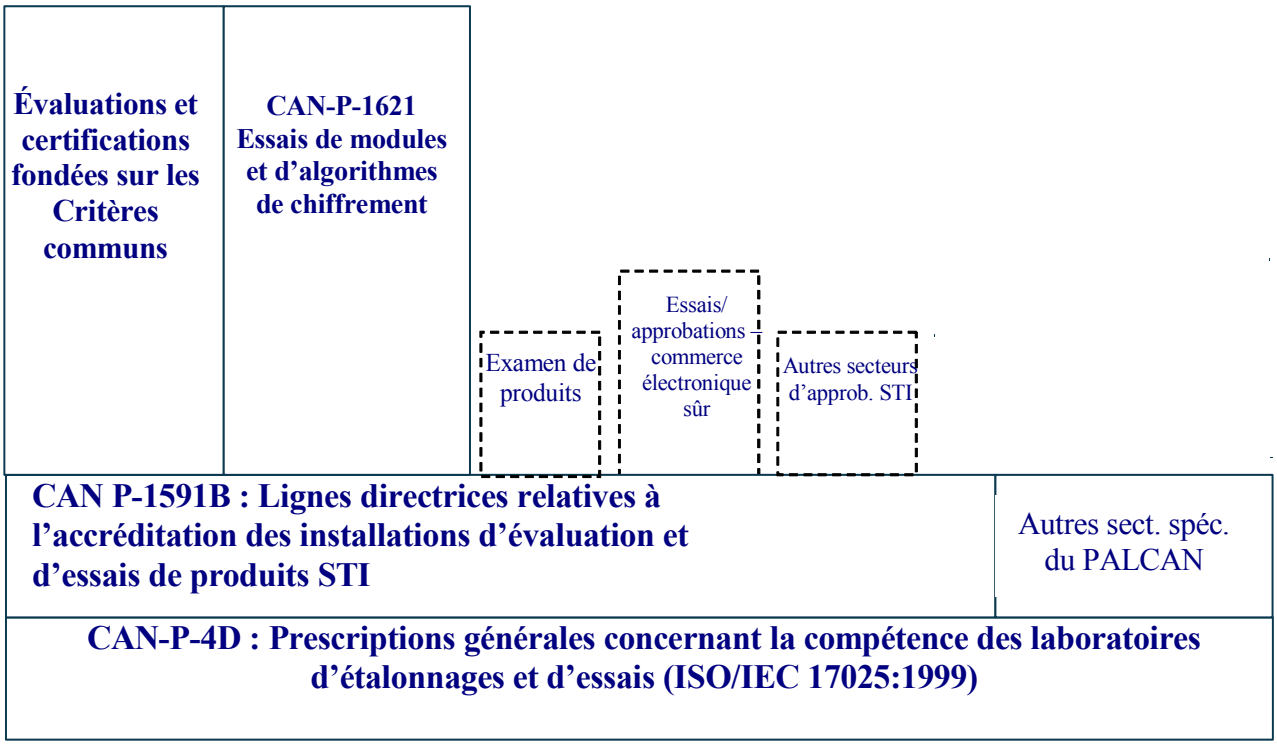

Figure 2 – Cadre d'accréditation du CCN

EXIGENCES GÉNÉRALES

Les installations d'essais qui souhaitent être accréditées en fonction du présent document doivent aussi répondre aux exigences des documents suivants :

a) Guide PALCAN, *Programme d'accréditation des laboratoires;*

b) CAN-P-4D : 2000, *Prescriptions générales concernant la compétence des laboratoires d'étalonnages et d'essais;*

c) CAN-P-1591B : 2001, *Lignes directrices relatives à l'accréditation des installations d'évaluation et d'essais de produits de sécurité des technologies de l'information.*

1. RÉFÉRENCES

1.1 Les documents de référence suivants s'appliquent à la présente norme et peuvent être obtenus auprès du CCN :

Guide PALCAN, *Programme d'accréditation des laboratoires*, Conseil canadien des normes

CAN-P-4D : 2000, *Prescriptions générales concernant la compétence des laboratoires d'étalonnages et d'essais*, Conseil canadien des normes

CAN-P-1510D : 2000, *Évaluation – Guide de cotation à utiliser avec le CAN-P-4D*, Conseil canadien des normes

CAN-P-1591B : 2001, *Lignes directrices relatives à l'accréditation des installations d'évaluation et d'essais de produits de sécurité des technologies de l'information*, Conseil canadien des normes

CAN-P-1592B : 2001, *Liste de contrôle applicable à l'évaluation des installations d'essais de produits de sécurité des technologies de l'information*, Conseil canadien des normes

CAN-P-1622 : 2001, *Liste de contrôle applicable à l'évaluation des installations d'essais de modules et d'algorithmes cryptographiques*, Conseil canadien des normes

Pour commander l'un de ces documents, prière de s'adresser au :

Conseil canadien des normes
270, rue Albert, bureau 200
Ottawa (Ontario) K1P 6N7
Canada
Tél. : (613) 238-3222
Fax : (613) 569-7808

Plusieurs de ces documents sont disponibles sur le site Web du CCN à l'adresse http://www.scc.ca/can_p/canplist.html.

1.2 Les documents de référence suivants s'appliquent à la présente norme et peuvent être obtenus auprès du bureau du National Voluntary Laboratory Accreditation Program (NVLAP) :

NIST Handbook 150, *NVLAP Procedures and General Requirements,* Édition 2001

NIST Handbook 150-17, *NVLAP Cryptographic Module Testing,* juin 2000

Pour commander les publications du NVLAP, prière de s'adresser au :

National Voluntary Laboratory Accreditation Program
National Institute of Standards and Technology
100 Bureau Drive, Stop 2140
Gaithersburg, Maryland
United States of America 20899-2140
Tél. : (301) 975-4016
Fax : (301) 926-2884
Courriel : nvlap@nist.gov

Il est aussi possible d'obtenir une copie des guides 150 et 150-17 du NIST sur le site Web du NVLAP à l'adresse : http://ts.nist.gov/nvlap.

1.3 Les documents de référence suivants s'appliquent à la présente norme et peuvent être obtenus auprès du National Institute of Standards and Technology/ Information Technology Laboratory (NIST/ITL) :

Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, mars 1995 (ci-après appelé *140-2:Derived Test Requirements*);

Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, mis à jour périodiquement (ci-après appelé *140-2:Implementation Guidance*);

CMVP Management Processes Manual (Ébauche);

Cryptographic Support Test Tool-Cryptik.

Progiciels contenant des essais et des méthodes d'essais pour algorithmes cryptographiques.

Pour commander les publications et les logiciels du NIST/ITL, prière de s'adresser au :

Information Technology Laboratory (ITL)
Cryptographic Module Validation Program
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, Maryland
United States of America 20899-8930
Tél. : (301) 975-2934
Fax : (301) 948-1233.

Il est aussi possible d'obtenir une copie des publications du NIST/ITL aux adresses Internet suivantes :

140-2:Derived Test Requirements : http://csrc.nist.gov/cryptval/140-2/140test1.htm.

140-2:Implementation Guidance : http://csrc.nist.gov/cryptval/140-2/1401ig.htm.

Pour obtenir les essais et les procédures d'essai pour algorithmes cryptographiques, veuillez vous rendre au site Web suivant : http://csrc.nist.gov/cryptval.

Pour obtenir une copie de la norme FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, prière de s'adresser au :

National Technical Information Service
5285 Port Royal Road
Springfield, Virginia
United States of America 22161

Tél. : (800) 553-6847
Fax : (703) 605-6900
Courriel : orders@ntis.fedworld.gov.

La norme FIPS PUB 140-2 est disponible sur le site Web suivant : http://csrc.nist.gov/cryptval.

2. DÉFINITIONS

2.1 Les définitions applicables aux fins du présent document englobent toutes les définitions du document CAN-P-4D (c'est-à-dire, laboratoire, laboratoire d'essai, laboratoire d'étalonnage, essai d'étalonnage, méthode d'étalonnage, méthode d'essai, vérification, système qualité, manuel qualité, étalon de référence, matériau de référence, matériau de référence certifié, traçabilité, essai d'aptitude, exigences en matière d'accréditation), du document CAN-P-1591B (c'est-à-dire, signataires autorisés, approbation, évaluateur, conception fonctionnelle, conformité, évaluation de la conformité, module cryptographique, évaluation, installation d'évaluation et d'essais de produits STI, installation, accréditation d'installation, conseils en matière d'interprétation, domaine d'approbation STI, personnel technique clé, évaluation sur place, produit, essai d'aptitude, archives, autorité compétente reconnue en matière de STI[1], sécurité, exigences de sécurité, spécialiste technique, examen technique, outils d'essai) et les définitions

[1] Le terme s'applique seulement dans le contexte du CAN-P1591B et pas dans celui du CAN-P-1621 ni du PVMC.

pertinentes du guide ISO 8402 (p. ex., assurance de la qualité, contrôle de la qualité), de même que les définitions suivantes propres au présent document :

CCN : Conseil canadien des normes. (*SCC*)

Cryptik : Le *Cryptographic Support Test Tool* (CSTT) défini ci-dessous.

CST : Centre de la sécurité des télécommunications (*CSE*)

CSTT : *Cryptographic Support Test Tool*, outil servant à consigner les résultats des essais de modules cryptographiques. Il s'agit de la base de données *Cryptik* contenant les essais élémentaires abstraits (désignée sous le nom de *base de données Cryptik*).

DTR : *Derived Test Requirements for FIPS PUB 140-2* (voir article 1.3)

Essais d'algorithmes cryptographiques : Évaluation des entrées et des sorties visant à déterminer si la réalisation est conforme aux spécifications. (*Cryptographic algorithm testing*)

FIPS : *Federal Information Processing Standard*

IG : *Implementation Guidance for FIPS PUB 140-2* (voir article 1.3)

Périmètre cryptographique : Périmètre contigu clairement défini délimitant les frontières physiques d'un module cryptographique et englobent le matériel, les logiciels et/ou les micrologiciels de ce module. (*Cryptographic boundary*)

PVMC : Programme de validation des modules cryptographiques géré conjointement par le NIST/ITL et le CST. (*CMVP*)

Validation : Processus administratif employé par le NIST/ITL et le CST pour établir le degré de conformité d'une réalisation aux exigences précisées. (*Validation*)

VMC : Validation d'un module cryptographique qui consiste à déterminer sa conformité à la norme FIPS PUB 140-2. (*CMV*)

3. PORTÉE D'ACCRÉDITATION

3.1 Le CAN-P-1621 précise quatre portées d'accréditation. Les installations d'essais qui souhaitent souscrire au PVMC doivent être accréditées en vertu de la portée 1, groupe 1, et de la portée 2. L'accréditation en vertu de la portée 1, groupe 2, et de la portée 1, groupe 3, est optionnelle.

3.2 Les quatre portées d'accréditation sont les suivantes :

Portée 1

NIST-CSTT:140-2; National Institute of Standards and Technology – *Cryptographic Support Test Tool* (CSTT) pour la norme FIPS 140-2, *Security Requirements for Cryptographic Modules*.

Groupe 1 — Toutes les méthodes d'essai dérivées de la norme FIPS 140-2 et précisées dans le CSTT, à l'exception de celles énumérées dans les groupes 2 et 3.

Groupe 2 — Méthodes d'essai pour la sécurité physique (niveau 4) dérivées de la norme FIPS 140-2, et précisées dans le CSTT.

Groupe 3 — Méthodes d'essai pour la sécurité logique (niveau 4) dérivées de la norme FIPS 140-2, et précisées dans le CSTT.

Portée 2 — Algorithmes cryptographiques approuvés en fonction de la norme FIPS (voir http://csrc.nist.gov/cryptval), tel que l'exige le document FIPS PUB 140-2.

4. DÉMONSTRATION DE LA COMPÉTENCE TECHNIQUE

4.1 Composition de l'équipe d'évaluation

4.1.1 L'accréditation d'une installation d'essai à la norme CAN-P-1621 n'est qu'une des méthodes de démonstration de compétence pour l'essai de conformité de modules cryptographiques reconnues par le PVMC. D'autres méthodes reconnues par le PVMC sont contenues dans le *CMVP Management Processes Manual*. Puisque le programme est géré conjointement par le CST et le NIST, des évaluateurs de ces deux organismes se joindront aux évaluateurs du CCN lors de l'évaluation sur place et des essais d'aptitude.

4.2 Préparation de l'évaluation sur place

4.2.1 Avant de procéder à l'évaluation sur place, les évaluateurs examineront le manuel qualité de l'installation et les résultats des essais d'aptitude. Cette documentation doit être fournie aux évaluateurs au moins 15 jours ouvrables avant la date fixée pour l'évaluation sur place. Tout problème décelé lors de l'examen de ces documents sera approfondi lors de l'évaluation.

4.3 Essais d'aptitude

4.3.1 Toutes les installations sont tenues de prendre part à des essais d'aptitude liés aux méthodes d'essais déterminées. Elles doivent avoir réussi les essais d'aptitude avant de pouvoir obtenir l'accréditation initiale, et doivent les réussir à nouveau périodiquement par la suite. Les installations désirant obtenir le renouvellement de leur accréditation doivent avoir pris part à tous les essais d'aptitude obligatoires durant la précédente période d'accréditation.

4.3.2 Les essais d'aptitude peuvent être composés de plusieurs parties et ce, pour permettre l'évaluation appropriée d'une installation. Leur raison d'être : évaluer la capacité d'une installation à produire des données d'essais pouvant être répétées et renouvelables. Des parties du processus d'essai peuvent être « mises en évidence » dans le cadre des essais d'aptitude, p. ex., l'analyse du logiciel, du matériel, des données, etc. L'équipe d'évaluateurs peut choisir l'une ou plusieurs des méthodes suivantes dans le cadre de la conduite des essais d'aptitude (le choix est laissé à sa discrétion) :

a) Questionnaire s'adressant à tout le personnel responsable des essais. Le questionnaire devra comporter des questions sur chaque méthode d'essai comprise dans chaque unité pour laquelle l'installation souhaite obtenir l'accréditation. Les questions mesureront la connaissance du personnel sur les méthodes d'essai, de même que sa capacité à mettre à l'essai un module cryptographique particulier en fonction d'une exigence particulière et à mettre à l'essai un algorithme en fonction d'une spécification;

b) Mise à l'essai d'un article spécialement conçu et comprenant une ou plusieurs fonctions conformes ou non à la norme FIPS PUB 140-2. L'installation doit trouver les éléments non conformes, les consigner et indiquer quelles exigences de la norme FIPS PUB 140-2 n'ont pas été respectées en raison de la présence des éléments non conformes;

c) Examen d'une machine à états-finis spécialement conçue et comprenant une ou plusieurs fonctions non conformes à la norme FIPS PUB 140-2. Par exemple, la machine peut indiquer qu'il existe une transition directe d'un état d'erreur à un état d'utilisateur. L'installation doit trouver les éléments non conformes, les consigner et indiquer quelles exigences de la norme FIPS PUB 140-2 n'ont pas été respectées en raison de la présence des éléments non conformes;

d) Démonstration de l'utilisation correcte du *Cryptographic Support Test Tool (Cryptik)*. L'installation doit être en mesure de prouver que tout le personnel approprié en comprend le fonctionnement et sait comment l'utiliser. Pour ce faire, l'évaluateur peut observer le personnel de l'installation pendant que celui-ci utilise *Cryptik*;

e) Capacité à produire un rapport, dans le format approuvé, dont le contenu est identique à celui produit avec le logiciel *Cryptik*;

f) Capacité à comprendre les résultats d'essais consignés dans le logiciel *Cryptik*.

4.3.3 L'évaluateur peut apporter lui-même les échantillons des essais d'aptitude à l'installation le jour prévu de l'évaluation sur place, ou bien les acheminer à l'installation avant cette date.

4.3.4 Les résultats des essais d'aptitude seront communiqués aux participants dans les documents et rapports appropriés. Tout problème décelé lors des essais devra faire l'objet de discussions avec le personnel de l'installation responsable de l'élaboration d'un plan pour résoudre ce problème.

4.4 Évaluation sur place

4.4.1 Les évaluateurs du CCN/CST/NIST auront habituellement besoin d'un à deux jours pour mener à bien l'évaluation sur place des installations d'essais de modules cryptographiques. Toutes les observations faites par les évaluateurs dans le cadre de l'évaluation sont considérées comme de l'information de nature délicate et confidentielle réservée à l'entreprise.

4.4.2 L'installation devra être prête à procéder à des démonstrations, avoir vérifié le bon fonctionnement de son équipement et être prête à subir une évaluation selon les exigences définies dans le présent document ainsi que dans les documents CAN-P-4C et CAN-P-1591B du CCN, et dans le manuel qualité de l'installation. Les évaluateurs s'efforceront de perturber le moins possible les habitudes de travail. Durant leur séjour sur place, ils auront besoin de temps et d'un lieu de travail pour pouvoir terminer l'évaluation de la documentation.

4.4.3 L'évaluateur se servira du document CAN-P-1622, *Liste de contrôle applicable à l'évaluation des installations d'essais de modules et d'algorithmes cryptographiques*, et de toute autre liste de contrôle pertinente tirée du CAN-P-4D et du CAN-P-1591B du CCN. Les listes de contrôle servent à s'assurer que l'évaluation est exhaustive et que les évaluateurs vérifient les mêmes éléments dans toutes les installations. Ces listes sont rédigées de façon à prévoir toutes les situations, de sorte que toutes les questions ne s'appliqueront pas systématiquement dans tous les cas. Par contre, l'évaluateur pourra déborder le cadre fixé par la liste de contrôle pour approfondir certains points techniques, si besoin est.

4.4.4 Voici le déroulement type d'une évaluation :

a) L'évaluateur rencontre la direction et le personnel cadre de l'établissement pour expliquer le but de l'évaluation sur place et fixer un échéancier. Les informations fournies par l'installation sur le formulaire de demande d'accréditation pourront être examinées à cette occasion. D'autres membres du personnel de l'installation pourront assister à la rencontre, à la discrétion du responsable de l'installation;

b) L'évaluateur demandera la contribution du responsable de l'installation pour fixer des rencontres avec les membres du personnel. L'évaluateur n'aura pas nécessairement besoin de s'entretenir avec tous les membres du personnel, mais il pourra vouloir rencontrer des représentants de tous les secteurs d'activités;

c) Les membres du personnel de l'installation ne devraient pas répondre aux questions pour lesquelles ils estiment ne pas posséder les compétences voulues. Le fait de savoir à qui s'adresser et où trouver la réponse peut habituellement constituer une réponse acceptable;

d) L'évaluateur examine le système qualité de l'installation, y compris le manuel qualité, les équipements, les registres d'entretien, les versions de logiciels, les procédures de tenue de dossiers, les procédures d'essai, les procès-verbaux d'essais, les titres et qualités du personnel, les plans et les dossiers de formation du personnel, les procédures de mise à jour de la documentation pertinente (comme le IG et la liste de produits validés) et les mesures prévues pour assurer la protection des informations de nature délicate du fournisseur ou des informations de fabrication;

e) L'évaluateur aura examiné au préalable le manuel qualité transmis au CCN avant l'évaluation sur place; il en approfondira les aspects voulus avec les membres du personnel nommés à cet effet avant de le remettre aux représentants de l'installation;

f) Au moins un membre du personnel de l'installation devra être accessible pour répondre aux questions de l'évaluateur; cependant l'évaluateur pourra, s'il le désire, examiner les documents par lui-même. Habituellement, il ne demandera pas à emporter de documents hors des lieux;

g) L'évaluateur vérifiera les renseignements relatifs au personnel, notamment les descriptions d'emploi, les curriculum vitae et les évaluations de rendement. L'installation n'a pas à mettre à la disposition de l'évaluateur de renseignements dont la divulgation porterait atteinte à la vie privée des membres de son personnel, comme des renseignements sur la rémunération, des renseignements d'ordre médical ou des rapports d'évaluation de rendement ne présentant pas de pertinence en vue de l'accréditation de l'installation. Un membre du personnel des ressources humaines de l'installation pourra être présent lors de l'examen des renseignements personnels;

h) L'évaluateur examinera l'équipement (matériel et logiciel) et les installations afin d'établir leur caractère adéquat, leur capacité, leur conformité aux spécifications, etc.;

i) Une séance de compte rendu est organisée avec le responsable de l'installation et les membres du personnel, à la fin de l'évaluation sur place, afin de leur faire part des résultats de l'évaluation. Cette séance permet de passer en revue les faiblesses observées, et de convenir des mesures correctives à adopter. L'évaluateur signalera à cette occasion les éléments qui devront être corrigés avant que l'accréditation puisse être accordée. Pour les autres correctifs à apporter, l'installation disposera de

30 jours pour fournir au CCN un échéancier prévoyant la mise en oeuvre de toutes les mesures correctives dans un délai de 90 jours. Les éléments qui auront été corrigés durant l'évaluation et toutes les recommandations formulées seront expressément consignées par l'évaluateur;

j) Les commentaires portant sur des améliorations possibles non répertoriées de façon expresse parmi les faiblesses devraient être examinés sérieusement par l'installation, mais le suivi à assurer à ce chapitre est laissé à la discrétion de l'installation. Tout désaccord entre l'installation et l'évaluateur doit être signalé au CCN, au CST et au NIST en vue d'un examen plus approfondi;

k) L'évaluateur rédige un rapport d'évaluation sur place présentant ses observations. Il joint au rapport des copies des listes de contrôle dûment remplies, puis le signe et demande au responsable de l'installation autorisé de faire de même. Des copies du rapport et des listes de contrôle sont fournies à l'installation pour ses dossiers.

4.5 Accréditation

4.5.1 La décision d'accorder ou de renouveler l'accréditation d'une installation n'est pas prise par l'équipe d'évaluateurs, mais plutôt par le CCN, conformément aux procédures décrites dans le *Guide du PALCAN*.

4.6 Refus, suspension et retrait de l'accréditation

4.6.1 Une installation peut voir son accréditation refusée, suspendue ou retirée si elle ne se conforme pas à toutes les exigences du CCN précisées dans le présent document, et dans les documents CAN-P-1591B et CAN-P-4D, notamment si elle ne corrige pas les irrégularités relevées ou ne participe pas aux activités liées aux essais d'aptitude.

5. EXIGENCES LIÉES AU CAN-P-1591B – DÉTAILS SUPPLÉMENTAIRES

5.1 Généralités

5.1.1 La présente section doit être consultée en parallèle avec le CAN-P-1591B. Elle fournit des conseils ou des détails supplémentaires concernant l'interprétation de certaines dispositions du CAN-P-1591B pour lesquelles des procédures particulières aux essais de modules et d'algorithmes cryptographiques devront être utilisées. Les numéros des sections visées du CAN-P-1591B sont indiqués entre crochets à la suite du titre de la rubrique.

5.2 Organisation [CAN-P1591B, article 5.2]

Aucune exigence supplémentaire.

5.3 Système qualité [CAN-P1591B, article 5.3]

5.3.1 Les exigences liées au système qualité sont conçues de façon à promouvoir l'adoption de pratiques propres à assurer l'intégrité technique de l'analyse, ainsi que l'adhésion à des pratiques d'assurance de la qualité appropriées à la validation de modules cryptographiques et aux évaluations de la conformité d'algorithmes cryptographiques.

5.3.2 L'installation doit tenir à jour un manuel qualité consignant de façon exhaustive les politiques, les pratiques et les modalités appliquées par l'installation pour assurer la qualité des évaluations de la conformité au PVMC.

5.3.3 Le manuel qualité et les documents connexes doivent contenir ou mentionner la documentation qui décrit et précise les procédures élaborées par l'installation en vue de répondre à toutes les exigences du présent document. Les évaluateurs du CCN passeront en revue cette documentation lors de l'évaluation sur place.

5.3.4 Les documents de référence, les normes et les publications pertinentes mentionnés à l'article 1 du présent document relativement au PVMC doivent être accessibles en vue de l'élaboration et du maintien du système qualité.

5.3.5 Afin de permettre au PVMC d'effectuer l'audit des aspects techniques des opérations d'une installation d'essai, il peut être nécessaire qu'un audit soit effectuer par le CCN ou une autre organisation appropriée peut être appelé à mener un audit externe, ou bien l'installation peut être appelée à fournir au NIST/ITL et au CST des rapports d'essais de validation ou à se soumettre à un interview par téléphone.

5.3.6 L'installation d'essai doit établir des procédures définissant l'évaluation à mener lorsque des changements, majeurs ou mineurs, sont apportés au logiciel *Cryptik* ou à d'autres outils d'essai. Cette mesure s'impose pour assurer, comme il se doit, l'harmonisation des procédures au sein des installations d'essais et la conformité à toutes les normes et spécifications. (Nota : les essais touchant des algorithmes cryptographiques non fournis par le NIST doivent être achetés par le biais des organismes rédacteurs de normes appropriés.)

5.3.7 Les procédures applicables en vue de la validation des outils d'essai et de l'utilisation de la base de données *Cryptik* doivent être consignées par l'installation.

5.4 Revue des demandes, appels d'offre et contrats [CAN-P-1591B article 5.4]

Aucune exigence supplémentaire.

5.5 Contrôle des archives [CAN-P1591B, article 5.5]

5.5.1 L'installation doit conserver des archives sur les éléments suivants; elles feront l'objet de vérifications au hasard dans le cadre de l'évaluation sur place :

a) versions et mises à jour de *Cryptik*;

b) documents *Cryptik*;

c) dossiers de correspondance comprenant les questions soumises, tels qu'ils sont définis dans le document *140-2:Implementation Guidance*, et les réponses fournies.

5.5.2 Les rapports d'essai générés au moyen de *Cryptik* et les valeurs d'essais définitifs pour l'algorithme évalué doivent être conservés par l'installation une fois les essais de durée de vie des modules cryptographiques terminés, ou selon les précisions du client.

5.6 Personnel [CAN-P1591B, article 5.6]

5.6.1 L'installation doit employer un personnel administratif et technique possédant les compétences voulues pour mener à bien des essais en vertu de la norme FIPS PUB 140-2 et évaluer la conformité des algorithmes cryptographiques.

5.6.2 L'installation doit tenir à jour les descriptions d'emploi et les curriculum vitae des membres du personnel qui occupent des postes dans le domaine des essais en vertu de la norme FIPS PUB 140-2 et de la mise à l'essai d'algorithmes cryptographiques, et des membres du personnel cadre.

5.6.3 L'installation doit consigner les compétences exigées pour chacun des postes dont les fonctions comprennent la validation de modules cryptographiques et l'évaluation de la conformité des algorithmes cryptographiques.

5.6.4 La formation s'adressant au personnel de l'installation doit porter sur les champs de compétence suivants :

a) exigences de nature générale liées aux méthodes d'essai, y compris à la production de rapports d'essai;

b) classes de plates-formes matérielles (pour algorithmes cryptographiques logiciels);

c) mesure des tensions et de la température [*Environmental Failure Protection/Environmental Failure Testing* (EFP/EFT), niveau 4 uniquement];

d) concepts liés à la sécurité informatique;

e) étude sur modèle de machines à états finis;

f) qualité de fabrication, techniques de sabotage et de détection des sabotages;

g) spécifications de conception de logiciel, y compris les langages évolués et les modèles formels;

h) techniques et concepts liés à la gestion des clés;

i) techniques liées au contrôle de l'interférence électromagnétique et de la compatibilité électromagnétique;

j) techniques d'auto-test cryptographiques;

k) algorithmes cryptographiques conformes à la norme FIPS;

l) concepts liés aux systèmes d'exploitation;

m) normes FIPS PUB traitant de cryptographie;

n) terminologie liée à la cryptographie et familles d'algorithmes cryptographiques;

o) Critères communs (ISO/IEC 15408:1999);

p) fonctionnement et maintenance de *Cryptik*;

q) Internet, logiciels liés à Internet, et capacité à trouver et à télécharger des documents de référence et des renseignements à partir du site Web du PVMC http://csrc.nist.gov/cryptval.

5.6.5 L'installation doit fournir une description officielle du programme de formation accessible aux nouveaux employés et aux employés en fonction. Le programme de formation doit porter notamment sur les champs de compétence présentés au paragraphe 5.6.4 ci-dessus.

5.6.6 Les membres du personnel en fonction doivent recevoir une formation supplémentaire dans les cas suivants : nouveau matériel et(ou) logiciel, approbation de nouveaux algorithmes cryptographiques, attribution de nouvelles fonctions, modification ou élaboration de normes FIPS traitant de cryptographie.

5.6.7 La formation doit notamment porter sur l'application de nouvelles méthodes d'essai, sur le document *140-2:Implementation Guidance* et sur la conduite d'essais.

5.7 Locaux et environnement [CAN-P1591B, article 5.7]

5.7.1 L'installation doit répondre aux exigences en matière de locaux et d'environnement propres aux essais menés dans le cadre du PVMC et à la mise à l'essai d'algorithmes cryptographiques, tels que précisés dans le DTR.

5.7.2 Une fonction de courrier électronique et l'accès à Internet sont exigés dans le cadre du PVMC.

5.7.3 Les rapports d'essai et les autres documents peuvent être acheminés au NIST/ITL et au CST par courrier électronique.

5.8 Méthodes d'essai et d'étalonnage et validation des méthodes [CAN-P1591B, article 5.8]

5.8.1 Lorsque des essais sont menés dans les locaux d'un client, seul le personnel de l'installation d'essais devra exécuter ou contrôler toutes les interventions voulues pour mener les essais et consigner les résultats, ce qui comprend le chargement, la compilation, la configuration et l'exploitation de *Cryptik*.

5.8.2 L'installation doit utiliser les méthodes d'essai décrites dans le document *140-2:Derived Test Requirements*; des précisions sont fournies dans le document *140-2:Implementation Guidance*. Lorsque des exceptions s'imposent pour des raisons de nature technique, le client doit en être avisé et les détails doivent être consignés dans le rapport d'essai. Il est important de bien documenter les exceptions par rapport à *Cryptik* pour assurer l'exactitude de l'assertion d'essai et de son interprétation. Ces rapports peuvent être utilisés pour mettre à jour *Cryptik* et les documents d'accompagnement.

5.8.3 L'installation doit utiliser les méthodes d'essai d'algorithmes cryptographiques et les essais connexes qui se trouvent sur le site Web http://csrc.nist.gov/cryptval.

5.9 Équipement [CAN-P1591B, article 5.9]

5.9.1 Pour les fins de la portée d'accréditation, les installations doivent disposer du matériel, du logiciel et des installations informatiques voulues pour effectuer la mise à l'essai de modules cryptographiques, y compris l'équipement d'essai et de mesure pour effectuer des essais physiques.

5.9.2 Les installations accréditées pour effectuer les méthodes d'essai de conformité de niveau 4 doivent posséder l'équipement et les renseignements suivants :

a) bloc d'alimentation;

b) chambre thermique; et

c) textes de modèle formel.

5.9.3 L'installation doit posséder, charger et exploiter une copie de *Cryptik* fournie par NIST/ITL, et produire un imprimé des résultats d'essais au moyen de la base de données *Cryptik*.

5.9.4 L'installation doit posséder une plate-forme informatique capable de charger et d'exploiter correctement une copie de *Cryptik* fournie par le NIST/ITL.

5.9.5 L'installation doit consigner les procédures relatives aux mesures suivantes associées au logiciel *Cryptik* : mises à jour, copie du logiciel original sur le support approprié et transfert des données de la base de données d'un site à un autre.

5.10 Traçabilité des mesures [CAN-P1591B, article 5.10

5.10.1 La traçabilité des essais élémentaires abstraits est assurée grâce à l'utilisation de *Cryptik*. La traçabilité aux exigences de la norme FIPS PUB 140-2 est assurée par les assertions et les DTR connexes consignés dans la base de données *Cryptik*. Les assertions sont des citations textuelles tirées de la norme FIPS PUB 140-2. Les DTR se divisent en deux groupes d'exigences : le premier visant le fournisseur, et l'autre l'évaluateur du module cryptographique.

5.10.2 L'équipement utilisé pour conduire les évaluations de la conformité doit être entretenu/réétalonné :

a) conformément aux recommandations du fabricant;

b) tel qu'il est précisé dans la méthode d'essai;

c) annuellement :

selon celle de ces périodes qui est la moins longue entre les étalonnages.

5.10.3 Il faut assurer la traçabilité à la plus récente version de *Cryptik* avant de mener des essais, soit par la gestion de la configuration du matériel et du logiciel, soit par le contrôle des versions.

5.10.4 Lorsqu'il y a écart entre les exigences de la norme FIPS PUB 140-2 et la base de données *Cryptik* contenant les essais élémentaires abstraits, l'installation doit démontrer le respect de la conduite de chaque essai élémentaire à la norme FIPS PUB 140-2, tout en conservant les constatations ou les mesures liées à chaque série d'observations.

5.11 Rapport sur les résultats [CAN-P1591B, article 5.11]

5.11.1 Les rapports d'essai remis aux clients doivent être conformes aux exigences contractuelles, de même qu'aux exigences de la norme FIPS PUB 140-2 et des documents CAN-P-4D et CAN-P-1591B.

5.11.2 Si l'installation ajoute dans le rapport d'essai des commentaires, des analyses ou des résultats supplémentaires qui ne répondent pas aux exigences de la norme FIPS PUB 140-2, elle doit préciser qu'il s'agit d'éléments qui dépassent la portée d'accréditation.

5.11.3 Les rapports d'essais à soumettre au PVMC doivent répondre aux exigences des documents *140-2:Derived Test Requirements* et *140-2:Implementation Guidance*, de même qu'aux exigences relatives à l'accréditation.

5.11.4 Les résultats d'essais relatifs aux algorithmes cryptographiques doivent inclure les valeurs produites par chaque algorithme évalué.

5.11.5 Outre les rapports imprimés, l'installation doit soumettre au NIST/ITL et au CST des rapports sur support électronique (comme une disquette). La version électronique doit être identique à la version imprimée et doit être produite au moyen d'un logiciel accepté par le NIST/ITL et le CST.

5.11.6 Les rapports produits au moyen de *Cryptik* sont reconnus tant que rapports d'essais en vertu du PVMC.

5.11.7 Les corrections et les ajouts à un rapport d'essai créé à des fins de validation et soumis au PVMC doivent être convenablement indiqués dans un document complémentaire conforme aux exigences du PVMC.