Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

INSTRUCTIONS DU PROGRAMME CANADIEN LIÉ AUX CRITÈRES COMMUNS

POUR LES PRATICIENS DES CRITÈRES COMMUNS

TLP:WHITE

Canada

Avant-propos

La publication *Instructions du Programme canadien lié aux Critères communs* est un document NON CLASSIFIÉ destiné aux laboratoires d'essais agréés en vertu du Programme canadien. Elle remplace toute instruction antérieure relative au Programme canadien lié aux Critères communs, ayant été émise par le Centre canadien pour la cybersécurité ou le Centre de la sécurité des télécommunications.

Date d'entrée en vigueur

La présente publication entre en vigueur le 15 juin 2022.

Historique des modifications

Version	Modifications	Date
1.0	Révision initiale d'un ensemble harmonisé d'instructions relatives au programme : - regroupement de toutes les instructions du Schéma en un seul document; - reformatage du document conformément au modèle du Centre canadien pour la cybersécurité; - mise à jour du contenu des instructions afin de tenir compte des changements apportés au processus.	30 septembre 2019
1.1	Révision de la section traitant des fonctionnalités cryptographiques.	11 juin 2021
1.2	Ajout des sections « Fonctionnalité de base » et « Fonctionnalité essentielle », « Tests effectués à distance » et « Évaluation et correction des vulnérabilités ».	25 octobre 2021
1.3	Révision de la section « Admissibilité des évaluations », ajout d'un document de référence pour la cryptographie approuvée, mise à jour des exigences relatives aux jalons des évaluations visant à retirer la confirmation de l'approbation obtenue du Centre pour la cybersécurité, modification de la date du jalon des tests à PiE + **4,5** mois, retrait de la proposition de tests à distance de l'étape d'admissibilité, harmonisation de la terminologie.	6 décembre 2021
1.4	Intégration des commentaires découlant de l'examen de l'organisme de certification.	31 décembre 2021
1.5	Mise à jour de la section Admissibilité.	7 janvier 2022
1.6	Mises à jour basées sur les commentaires formulés par les laboratoires d'essais.	21 février 2022

1.7	Mises à jour basées sur les commentaires formulés par les laboratoires d'essais.	25 mars 2022
1.8	Changements de mise en forme	8 juin 2022

Vue d'ensemble

Le présent document contient toutes les instructions relatives aux évaluations effectuées en vertu du Programme canadien lié aux Critères communs.

Table des matières

1 Introduction 5

2 Admissibilité des évaluations 6

3 Fonctionnalités de base et essentielle 7

3.1 Fonctionnalité de base 7

3.2 Fonctionnalité essentielle 7

3.3 Spécification des exigences 7

4 Échéanciers des évaluations 8

4.1 Jalons des évaluations 8

4.1.1 Jalon de la cible de sécurité 8

4.1.2 Jalon de la conception et de l'entropie 8

4.1.3 Jalon des tests 8

4.1.4 Jalon de l'évaluation finale 8

4.2 Délais prescrits pour les jalons 9

4.3 Demande de prolongation des délais prescrits pour les jalons 9

4.4 Non-respect des délais prescrits pour les jalons 9

5 Évaluation des fonctionnalités cryptographiques 10

5.1 Fonctionnalité cryptographique 10

5.2 Vérification des versions cryptographiques 10

5.3 Évaluation d'entropie 10

6 Tests effectués à distance 11

6.1 Conditions 11

6.2 Exigences 11

7 Évaluation et correction des vulnérabilités 12

7.1 Évaluation 12

7.2 Correction 12

8 Contenu complémentaire 13

8.1 Abréviations, acronymes et sigles 13

8.2 Références 13

1 Introduction

Les *Critères communs pour l'évaluation de la sécurité des technologies de l'information* (aussi appelés Critères communs ou CC) sont une norme internationale qui permet de préciser les exigences de sécurité des produits de technologies de l'information (TI). Le Centre canadien pour la cybersécurité (ci-après appelé le Centre pour la cybersécurité) agit à titre d'organisme de certification (OC) pour les évaluations selon les Critères communs effectuées au Canada.

Le présent document procure aux centres d'évaluation selon les Critères communs (ci-après appelés laboratoires d'essais) de plus amples détails sur les évaluations réalisées en vertu du programme canadien. Pour obtenir de l'information générale sur le Programme canadien lié aux Critères communs, prière de visiter le site Web des Critères communs du Centre de la cybersécurité.

2 Admissibilité des évaluations

Le Centre pour la cybersécurité accepte les évaluations en vertu du programme des Critères communs dans l'ordre de priorité suivant :

1. Les évaluations des profils de protection en vertu des Critères communs, notamment :
   - les *profils de protection collaborative* internationaux élaborés par la communauté technique internationale;
   - les versions évoluées et les profils de protection sélectionnés élaborés par l'un des pays membres de *l'Arrangement relatif à la reconnaissance des certificats liés aux Critères communs du domaine de la sécurité des technologies de l'information* (en anglais seulement), également appelé *Arrangement de reconnaissance des Critères communs* ou ARCC;
2. Les types de technologies qui ne conviennent pas aux profils de protection (autres évaluations prises en compte dans la portée de l'*Arrangement de reconnaissance des Critères communs* [ARCC]). Au moment de rédiger le présent document, ces évaluations pouvaient atteindre le niveau d'assurance (EAL pour *Evaluation Assurance Level*) 2.

Le Centre pour la cybersécurité pourra également envisager au cas par cas s'il convient d'accepter des évaluations qui outrepassent la portée de l'ARCC, notamment les évaluations avec un niveau d'assurance EAL 3 ou EAL 4.

3 Fonctionnalités de base et essentielle

Pour les évaluations conformes au niveau d'assurance de l'évaluation (EAL pour *Evaluation Assurance Level*), où les spécifications des exigences fonctionnelles de sécurité (SFR pour *Security Functional Requirement*) ne sont pas prédéterminées dans un profil de protection, il est important de veiller à ce que l'évaluation aborde un ensemble pertinent de fonctionnalités de sécurité. Cela comprend la *fonctionnalité de base* et la *fonctionnalité essentielle* décrites ci-dessous.

3.1 Fonctionnalité de base

Par fonctionnalité de base, on entend l'objectif principal d'un produit, ce qu'un consommateur peut s'attendre à voir inclure dans la portée de l'évaluation et la façon dont il est mis en marché. Il pourrait être nécessaire de créer des SFR étendues dans les cas où la fonctionnalité de base de la cible d'évaluation (TOE pour *Target of Evaluation)* ne peut être représentée par les SFR existantes. Toute fonctionnalité de base incluse devrait concerner la cybersécurité d'une quelconque manière (par opposition à une fonctionnalité qui n'a rien à voir avec la cybersécurité).

3.2 Fonctionnalité essentielle

Par fonctionnalité essentielle, on entend une fonctionnalité que le Centre pour la cybersécurité juge importante pour la cybersécurité du produit (selon la nature de la TOE), comme la gestion sécurisée et la communication inter-TOE.

3.3 Spécification des exigences

Les évaluations sont nécessaires pour inclure la fonctionnalité de base dans la TOE et toute fonctionnalité essentielle incluse (ou l'absence d'une telle fonctionnalité). Il incombe d'ailleurs au laboratoire d'essais de fournir une justification pour toute lacune relevée.

4 Échéanciers des évaluations

Le Centre pour la cybersécurité reconnaît qu'il est impératif que l'évaluation soit effectuée en temps opportun, puisque les clients sont tenus de fournir l'assurance de la sécurité des versions actuelles de leurs produits de TI. Par conséquent, il est important que la durée d'évaluation des produits tienne compte du raccourcissement des cycles de vie des produits modernes.

Le Centre pour la cybersécurité estime que les évaluations modernes reposent sur une préparation rigoureuse des évaluations, notamment l'analyse fonctionnelle des lacunes et les tests fonctionnels préliminaires. C'est pourquoi il a mis en place des jalons et des échéanciers auxquels les laboratoires d'essais devront se conformer au moment d'effectuer les évaluations.

4.1 Jalons des évaluations

Le Centre pour la cybersécurité reconnaît les jalons d'évaluation suivants :

1. Cible de sécurité;
2. Conception et entropie;
3. Tests;
4. Évaluation finale.

4.1.1 Jalon de la cible de sécurité

Pour se conformer au jalon de la cible de sécurité, le laboratoire d'essais doit réaliser toutes les activités d'évaluation associées à la classe d'assurance *Évaluation d'une cible de sécurité* (voir la section 12 de la référence [1]).

Une fois le jalon de la ST atteint, le Centre pour la cybersécurité ajoute le produit à la liste des produits en cours d'évaluation du Programme lié aux CC. La date stipulée dans la liste Produit en cours d'évaluation (PiE pour *Product in Evaluation*) correspondra à la date d'ajout du produit en question.

4.1.2 Jalon de la conception et de l'entropie

Pour se conformer au jalon de la conception et de l'entropie, le laboratoire d'essais doit réaliser toutes les activités d'évaluation associées à la classe d'assurance *Développement* (voir la section 13 de la référence [1]) et une analyse de l'entropie dès lors qu'une telle analyse est nécessaire pour se conformer au profil de protection (PP) mentionné.

4.1.3 Jalon des tests

Pour se conformer au jalon des tests, le laboratoire d'essais doit procéder à tous les tests fonctionnels et de pénétration requis.

4.1.4 Jalon de l'évaluation finale

Pour se conformer au jalon de l'évaluation finale, le laboratoire d'essais doit réaliser toutes les activités d'évaluation.

4.2 Délais prescrits pour les jalons

Le Centre pour la cybersécurité impose les délais suivants aux jalons d'évaluation décrits à la section 4.1 :

Jalon	Échéance
Conception et entropie	Date PiE + 2 mois
Tests	Date PiE + 4,5 mois
Évaluation finale	Date PiE + 6 mois

Pour s'assurer que le Centre pour la cybersécurité a suffisamment de temps pour passer en revue les livrables de l'évaluation finale, on doit lui faire parvenir ces livrables au plus tard dans les deux semaines précédant les délais prescrits pour le jalon.

4.3 Demande de prolongation des délais prescrits pour les jalons

Le Centre pour la cybersécurité considérera les demandes transmises par les laboratoires d'essais pour obtenir une prolongation délais prescrits pour les jalons. Le laboratoire d'essais doit expliquer en détail la raison pour laquelle il ne peut respecter l'échéance, proposer une période de prolongation raisonnable et décrire les mesures qu'il prendra pour se conformer à cette nouvelle échéance.

4.4 Non-respect des délais prescrits pour les jalons

Le Centre pour la cybersécurité retirera de la liste des produits en cours d'évaluation tout produit de TI dont l'évaluation ne respecte pas les délais prescrits pour le jalon de la conception et de l'entropie. Cela dit, le laboratoire d'essais pourra continuer l'évaluation, qui demeurera admissible aux fins de certification, dans la mesure où il respecte les délais prescrits pour le jalon de l'évaluation finale.

Le Centre pour la cybersécurité considérera l'évaluation comme étant non admissible à la certification si elle ne respecte pas les délais prescrits pour le jalon de l'évaluation finale. Les laboratoires d'essais devront soumettre une nouvelle demande d'admissibilité.

5 Évaluation des fonctionnalités cryptographiques

Le Centre pour la cybersécurité se base sur les résultats du Programme de validation des modules cryptographiques (PVMC) et du Programme de validation des algorithmes de chiffrement (CAVP pour *Cryptographic Algorithm Validation Program*, en anglais seulement) pour veiller à ce que les évaluateurs puissent évaluer correctement les modules cryptographiques et les algorithmes visés par l'évaluation.

Remarque : Le Centre pour la cybersécurité gère le PVMC et le CAVP en partenariat avec le National Institute of Standards and Technology (NIST) des États-Unis.

5.1 Fonctionnalité cryptographique

- Évaluations de conformité au PP : un certificat du CAVP est requis pour la cryptographie mentionnée.
- Évaluations de conformité au EAL dont l'objectif principal de la TOE est la cryptographie : un certificat du PVMC est requis pour la cryptographie mentionnée.
- Évaluations de conformité au EAL dont l'environnement offre la cryptographie nécessaire à la prise en charge de la fonctionnalité de la TOE : un certificat du PVMC est requis pour la cryptographie mentionnée.
- Évaluations de conformité au EAL où la cryptographie est utilisée pour prendre en charge la fonctionnalité : un certificat du CAVP peut être utilisé pour la cryptographie mentionnée. Dans certaines conditions, la mise à l'essai au moyen d'une implémentation valide connue peut être acceptable plutôt que le CAVP.

Dans tous les cas, seule la cryptographie approuvée par le Centre pour la cybersécurité doit être utilisée. La publication suivante aborde et décrit les algorithmes de chiffrement approuvés et les méthodes qu'il convient d'utiliser : https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b.

5.2 Vérification des versions cryptographiques

Le Centre pour la cybersécurité demande aux évaluateurs de vérifier la présence de toutes les versions cryptographiques mentionnées par le fournisseur. Les laboratoires d'essais ne peuvent se contenter de faire mention du certificat du CAVP ou du PVMC. Cette vérification peut s'effectuer de différentes façons selon le type de version et les accès aux fonctions sous-jacentes de la TOE qui ont été accordés à l'évaluateur.

5.3 Évaluation d'entropie

Le Centre pour la cybersécurité exige qu'une évaluation d'entropie soit réalisée dès que l'on fait mention d'une annonce de conformité à un profil de protection comportant des exigences relatives à la génération de nombres aléatoires par la TOE. Ces profils de protection énoncent clairement les cas où la cible de sécurité doit mentionner les fonctions de génération de nombres aléatoires.

Il est inutile de procéder à une telle évaluation si la portée de l'évaluation de la cible de sécurité ne comporte aucune exigence de génération de nombres aléatoires.

6 Tests effectués à distance

On s'attend à ce que les laboratoires d'essais testent les produits dans leurs installations. Dans des circonstances exceptionnelles, il pourrait être impossible de le faire. Vous trouverez ci-dessous les conditions dans lesquelles les laboratoires d'essais sont autorisés à tester les produits à distance et les exigences qu'il leur faudra respecter.

6.1 Conditions

Dans des circonstances exceptionnelles, les laboratoires d'essais peuvent demander d'effectuer des tests à distance s'ils se trouvent dans les situations suivantes :

- Si les coûts associés à la mise à l'essai, à l'expédition et à la configuration de la TOE sont prohibitifs;
- Si la configuration ou l'environnement de la TOE est extrêmement complexe et exige un soutien considérable du développeur;
- Si la mise à l'essai exige des outils ou de l'équipement spécialisés que le fournisseur possède, mais ne peut fournir au laboratoire d'essais;
- Autres conditions sujettes à l'approbation du Centre pour la cybersécurité.

6.2 Exigences

Pour obtenir l'approbation du Centre pour la cybersécurité d'effectuer des tests à distance, le laboratoire d'essais doit fournir les détails suivants :

- une justification détaillée :
  - si on soulève la question des coûts, fournir une ventilation générale des coûts associés;
  - si on soulève la question de la complexité, expliquer pourquoi l'environnement ou la configuration de la TOE est extrêmement complexe;
  - si on soulève l'obligation d'utiliser des outils spécialisés, fournir les détails relatifs aux outils et la raison pour laquelle le laboratoire d'essais ne peut pas se les procurer;
- une explication de la façon dont l'évaluateur se conformera aux exigences de AGD_PRE;
- comment l'évaluateur effectuera les tests;
- comment l'évaluateur assurera le contrôle continu de l'environnement;
- les mesures qui seront prises pour garantir la présence de témoins.

Le Centre pour la cybersécurité accorde l'approbation finale pour toutes les demandes de tests à distance.

7 Évaluation et correction des vulnérabilités

Les produits de TI pour lesquels un certificat des Critères communs est délivré ne doivent pas contenir de vulnérabilités non corrigées connues touchant la sécurité.

7.1 Évaluation

Toutes les vulnérabilités potentielles relevées durant la recherche dans le domaine public ou le processus automatisé de découverte basés sur des outils doivent être évaluées par le laboratoire d'essais selon les critères établis par le Centre pour la cybersécurité. Le processus d'évaluation doit être suffisamment détaillé pour déterminer si le produit et ses composants sont exempts de vulnérabilités touchant la sécurité.

7.2 Correction

Il est impératif de corriger toute vulnérabilité réelle qui a été relevée dans le produit évalué. S'il existe un correctif du fournisseur permettant de corriger la vulnérabilité, ce correctif doit être appliqué. Si le fournisseur n'offre aucun correctif, on peut gérer les vulnérabilités en adoptant une des approches suivantes :

- supprimer la fonctionnalité touchée (**option privilégiée**);
- désactiver la fonctionnalité touchée et publier un avis public expliquant le problème;
- présenter le plan adopté par le fournisseur pour corriger la vulnérabilité.

Le Centre pour la cybersécurité accorde l'approbation finale pour toutes les approches adoptées pour corriger les vulnérabilités.

8 Contenu complémentaire

8.1 Abréviations, acronymes et sigles

Terme	Définition
ARCC	Arrangement relatif à la reconnaissance des certificats liés aux Critères communs
CAVP	Programme de validation des algorithmes cryptographiques (*Cryptographic Algorithm Validation Program*)
CC	Critères communs
CST	Centre de la sécurité des télécommunications
EAL	Niveau d'assurance de l'évaluation (*Evaluation Assurance Level*)
GC	Gouvernement du Canada
NIST	National Institute of Standards and Technology
OSP	Politiques de sécurité organisationnelles (*Organizational Security Policy*)
PiE	Produit en cours d'évaluation (*Product in Evaluation*)
PP	Profil de protection
PVMC	Programme de validation des modules cryptographiques
RNG	Génération de nombres aléatoires (*Random Number Generation*)
SFR	Exigence fonctionnelle de sécurité (*Security Functional Requirement*)
ST	Cible de sécurité (*Security Target*)
STI	Sécurité des technologies de l'information
TI	Technologies de l'information
TOE	Cible d'évaluation (*Target of Evaluation*)

8.2 RÉFÉRENCES

Numéro	Référence
[1]	Critères communs. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*. Accessible au https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf (en anglais seulement).