Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Clauses contractuelles recommandées pour la cryptographie

Gestionnaires

TLP:CLEAR

Canada

Avant-propos

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour de plus amples renseignements, veuillez communiquer avec le Centre pour la cybersécurité :

- Courriel : contact@cyber.gc.ca
- Téléphone : 613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur en 19 septembre 2025.

Historique des révisions

Révision	Modifications	Date
1	Première version.	19 septembre 2025

D97-4/00-501-2025F-PDF
ISBN 978-0-660-78903-3

Vue d'ensemble

Si votre organisation a de plus en plus recours à la cryptographie pour protéger les infrastructures et les données, vous devez vous assurer que votre organisation se procure des produits et des services qui fournissent une protection efficace. Dans le cadre de l'achat d'un produit à usage unique ou de la conclusion d'un contrat avec un fournisseur de services tel qu'un fournisseur de services infonuagiques (FSI), votre organisation doit prendre en considération différents éléments pour s'assurer que le produit ou le service répondra aux besoins établis. La présente publication fournit des avis et des conseils sur les aspects dont il faut tenir compte lors de l'achat de produits et de services qui utilisent la cryptographie, notamment des exemples de clauses.

Table des matières

1 Introduction

Les conseils énoncés dans cette publication soulignent les facteurs de sécurité importants que votre organisation doit considérer pour l'achat de produits et services ayant recours à la cryptographie, ce qui comprend par exemple les fournisseurs de services et les fournisseurs de services infonuagiques (FSI).

Bien que les fournisseurs puissent présenter des conditions de base, l'équipe de direction de votre organisation est responsable de démontrer et de vérifier que les conditions générales d'utilisation et que les clauses relatives à la sécurité du contrat répondent aux besoins en matière de sécurité opérationnelle de votre organisation.

Les conditions générales d'utilisation doivent pouvoir s'adapter aux modifications futures afin de protéger les intérêts de votre organisation. Les conditions générales d'utilisation énoncées dans le contrat de service devraient également fournir à votre organisation les meilleurs résultats opérationnels possibles. Votre organisation doit prendre des mesures proactives pour veiller à ce que les dispositions de service comprennent des mécanismes de cybersécurité pour établir, communiquer, atténuer et prévenir les risques.

Cette publication présente les éléments liés à la cryptographie qui doivent être pris en considération, de même que les aspects fonctionnels et juridiques de l'approvisionnement lorsque les organisations travaillent avec des fournisseurs.

Les clauses décrites dans la présente publication ne doivent pas être considérées comme des conseils juridiques. Elles servent plutôt à offrir un meilleur contexte à votre organisation et à lui permettre de déterminer les points importants et les questions à poser lors de l'achat de produits et services cryptographiques.

1.1 Portée

Le Centre pour la cybersécurité offre des avis et des conseils à propos de la sélection et de l'utilisation d'algorithmes cryptographiques afin de protéger l'authenticité, la confidentialité et l'intégrité de l'information sensible. Cette publication propose des avis et des conseils sur les points à considérer lors des interactions avec un fournisseur dans le but d'acheter des produits ou des services qui utilisent la cryptographie pour protéger de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

Avis de non-responsabilité : Le Centre de la sécurité des télécommunications Canada (CST) et son Centre pour la cybersécurité ne recommandent ni n'approuvent l'utilisation d'aucune clause contractuelle particulière énumérée dans la présente publication. Les exemples de clauses contractuelles fournis peuvent être utiles pour l'achat de produits et services qui utilisent la cryptographie et sont donc offerts à titre d'information seulement. Nous recommandons de solliciter des conseils juridiques et d'approvisionnement lors de l'utilisation de ces clauses afin de vous assurer qu'elles répondent aux exigences de votre organisation.

2 Considérations relatives à la cryptographie

Pour protéger la confidentialité, l'intégrité et l'authenticité des données de votre organisation, vous devez vous assurer que toutes les infrastructures utilisent de manière efficace des mécanismes robustes de cryptographie dans les environnements locaux et dans les environnements des fournisseurs de services, y compris les environnements en nuage.

Les sections suivantes présentent les points à considérer lors de vos interactions avec les fournisseurs. Ces points comprennent les algorithmes, les modules et les paramètres cryptographiques permettant d'aider les organisations à suivre les conseils du Centre pour la cybersécurité.

La section 2.1 Facteurs à considérer pour les produits énonce les points importants à prendre en compte lors de l'achat de produits et accorde une grande importance aux exigences des produits en cause. La section 2.2 Facteurs à considérer pour les fournisseurs de services et de services infonuagiques fournit des avis et des conseils pour les interactions avec les fournisseurs de services, y compris les fournisseurs de services infonuagiques, et met l'accent sur la façon dont les fournisseurs sélectionnent, configurent et utilisent la cryptographie.

2.1 Facteurs à considérer pour les produits

Cette section présente les facteurs à considérer en ce qui a trait aux produits ainsi que des exemples de clauses contractuelles pouvant être utilisés lors de l'achat de produits prenant en charge la cryptographie. Les clauses ont été mises au point pour des produits dotés de modules cryptographiques intégrés, comme les réseaux privés virtuels (RPV) et d'autres dispositifs réseau offrant une prise en charge native de la cryptographie. Ces facteurs à considérer peuvent aussi servir à élaborer des exigences pour des appareils informatiques génériques sur lesquels des logiciels sont installés après l'achat (par exemple, des serveurs).

Remarque : La publication du Centre pour la cybersécurité Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111) est mise à jour régulièrement pour refléter les changements apportés aux avis et conseils en la matière. Toute clause servant à l'achat de produits et qui fait référence au document ITSP.40.111 devrait préciser la version de la publication.

2.1.1 Algorithmes cryptographiques recommandés

Les clauses contractuelles doivent s'assurer que les modules cryptographiques utilisent les algorithmes recommandés dans la publication ITSP.40.111 qui répondent aux exigences de vos systèmes. De plus, afin d'éviter les coûts supplémentaires durant la migration vers la cryptographie post-quantique (CPQ), nous recommandons que tous les nouveaux modules cryptographiques achetés prennent en charge les algorithmes CPQ appropriés.

Les clauses suivantes tiennent compte du fait que certains fournisseurs ne prennent pas actuellement en charge la CPQ et que certaines normes qui utiliseront les algorithmes peuvent encore être en cours d'élaboration. En précisant une date à laquelle le fournisseur doit fournir des capacités CPQ, votre organisation peut acheter le produit du fournisseur sans devoir attendre que celui-ci propose des produits prenant en charge la CPQ. Le fournisseur sera toutefois tenu de fournir des mises à niveau des modules cryptographiques avant ou à la date précisée.

Exemple de structure et de libellé de clause

- Les modules cryptographiques doivent utiliser seulement les algorithmes de chiffrement approuvés par le CST ainsi que les tailles de paramètres de chiffrement et les longueurs de clés établies dans la publication Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111).
- D'ici la fin de l'année 2026, les modules cryptographiques mettant en œuvre des mécanismes d'établissement de clé doivent prendre en charge la cryptographie post-quantique appropriée et conforme à la publication Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111).
- D'ici la fin de l'année 2026, les modules cryptographiques mettant en œuvre des mécanismes de signature numérique doivent prendre en charge la cryptographie post-quantique appropriée et conforme à la publication Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111).

2.1.2 Agilité cryptographique

L'utilisation de systèmes qui assurent l'agilité cryptographique permet aux organisations de reconfigurer ou de mettre à niveau des technologies cryptographiques, au besoin. Cet avantage est important, car les avancées dans la recherche sur la cryptographie et les vulnérabilités, ainsi que les méthodes de calcul, peuvent mener à des déploiements cryptographiques moins robustes par rapport à ce qui avait été établi lors du déploiement initial. Les produits doivent fournir des capacités permettant de modifier des paramètres, comme la longueur des clés, les tailles de paramètres et la durée de vie des clés, ainsi que de sélectionner des algorithmes de chiffrement sans la nécessité de remplacer des composants logiciels ou matériels. Ces capacités réduiront à la fois les dépenses et le temps nécessaire pour les achats associés aux nouvelles infrastructures. Les produits doivent également disposer de la capacité critique d'appliquer les correctifs nécessaires de manière sécurisée aux systèmes utilisant la cryptographie afin de s'assurer que les vulnérabilités sont atténuées après leur découverte.

Pour plus de détails sur l'agilité cryptographique, lisez la publication Conseils sur la mise en œuvre de l'agilité cryptographique (ITSAP.40.018).

Exemple de structure et de libellé de clause

- Les modules cryptographiques doivent prendre en charge l'agilité cryptographique en fournissant des algorithmes de chiffrement, des tailles de paramètres, des longueurs de clés et des cryptopériodes configurables.
- Les modules cryptographiques doivent prendre en charge les correctifs et les mises à jour signés par le fournisseur.

2.1.3 Certification cryptographique

Nous recommandons que tous les modules cryptographiques soient validés dans le cadre du Programme de validation des modules cryptographiques (PVMC). Le PVMC est géré conjointement par le Centre pour la cybersécurité et le National Institute of Standards and Technology (NIST), ce qui permet d'assurer que les fournisseurs mettent en œuvre correctement la cryptographie dans leurs produits et qu'ils respectent les pratiques exemplaires de sécurité recommandées par le Centre pour la cybersécurité. Afin de trouver des modules validés, les organisations peuvent effectuer une recherche dans la base de données des modules validés du PVMC qui est hébergée par le NIST. Les algorithmes de chiffrement utilisés dans les modules doivent être validés par le Programme de validation des algorithmes cryptographiques (PVAC) (en anglais seulement).

La certification du PVMC s'applique aux détails fournis dans la stratégie de sécurité qui est accessible sur la page Web du certificat du produit. Il est important que les produits utilisent le module cryptographique conformément à cette stratégie de sécurité, ce qui permet d'assurer avec un niveau élevé de certitude que le module fournira les services de sécurité attendus d'une manière prévisible.

Exemple de structure et de libellé de clause

- Les algorithmes de chiffrement doivent être validés par le Programme de validation des algorithmes cryptographiques (PVAC) et être associés à un certificat figurant dans la liste de validation du PVAC (en anglais seulement).
- Les modules cryptographiques doivent être validés par le Programme de validation des modules cryptographiques (PVMC) et être associés à une certification active du PVMC ainsi qu'à un numéro de certificat figurant dans la liste des modules validés par le PVMC (en anglais seulement).
- Les modules cryptographiques doivent être appliqués conformément à la stratégie de sécurité des modules cryptographiques figurant dans la liste des modules validés par le PVMC (en anglais seulement), en mode approuvé ou en mode autorisé.

2.2 Facteurs à considérer pour les fournisseurs de services et de services infonuagiques

Les organisations qui externalisent leur infrastructure TI ou leur gestion de solutions logicielle à des fournisseurs de services infonuagiques ou à des fournisseurs de services doivent tenir compte du type de cryptographie servant à la protection de l'information. La présente section fournit des éléments supplémentaires à prendre en compte lors de l'embauche d'un fournisseur de services ou d'un fournisseur de services infonuagiques.

Votre organisation doit s'assurer que les exigences contractuelles obligent l'entrepreneur à maintenir les systèmes TI conformément aux conseils cryptographiques en vigueur. En plus de la présente publication, le document du Centre pour la cybersécurité intitulé Clauses contractuelles recommandées en matière de cybersécurité pour les services infonuagiques (ITSM.50.104) présente des clauses générales d'approvisionnement et des facteurs à considérer lors de l'achat de solutions ou de services infonuagiques.

Remarque : Nous recommandons que les contrats avec des fournisseurs de services permettent d'assurer que les entrepreneurs respectent la dernière version de l'ITSP.40.111 et des Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062). Ainsi, les clauses qui font référence à l'ITSP.40.111 ou à l'ITSP.40.062 ne doivent pas mentionner une version particulière ou une date de publication précise, mais plutôt exiger que les entrepreneurs restent alignés sur les recommandations en vigueur du Centre pour la cybersécurité.

2.2.1 Cryptographie post-quantique

Nous recommandons que tous les modules cryptographiques prennent en charge les algorithmes CPQ approuvés par le CST dès que ceux-ci seront disponibles. Les clauses suivantes permettent aux organisations d'effectuer des achats auprès de fournisseurs de services en fonction de leurs besoins actuels, en s'assurant que les modules cryptographiques seront migrés pour prendre en charge la CPQ avant une date établie. Cette approche offre plus de flexibilité à l'acheteur et au fournisseur, tout en assurant une migration vers la CPQ qui ne sera pas retardée ou plus chère que prévu.

Exemple de structure et de libellé de clause

- D'ici la fin de l'année 2026, les modules cryptographiques mettant en œuvre des mécanismes d'établissement de clé doivent prendre en charge la cryptographie post-quantique appropriée et conforme à la publication Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111).
- D'ici la fin de l'année 2026, les modules cryptographiques mettant en œuvre des mécanismes de signature numérique doivent prendre en charge la cryptographie post-quantique appropriée et conforme à la publication Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111).

2.2.2 Configuration

La cryptographie doit être configurée conformément aux avis et aux conseils fournis dans les publications ITSP.40.111 et ITSP.40.062du Centre pour la cybersécurité. Le respect de la version la plus récente de ces publications aidera à assurer la protection de vos environnements à mesure que les conseils en matière de cryptographie évoluent. De plus, nous recommandons que le chiffrement soit configuré et exécuté en mode approuvé ou autorisé, selon la stratégie de sécurité du PVMC.

Exemple de structure et de libellé de clause

L'Entrepreneur doit :

- configurer les systèmes afin d'utiliser uniquement les algorithmes de chiffrement approuvés par le CST ainsi que les tailles de paramètres de chiffrement et les longueurs de clés établies dans les publications Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111) et Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062);
- s'assurer que ces politiques demeurent conformes aux versions subséquentes des publications.

2.2.3 Utilisation de modules et d'algorithmes cryptographiques validés

Semblable à la section 2.1.3 Certification cryptographique à propos de l'achat de produits, nous recommandons que seuls les algorithmes et les modules ayant été validés par le PVAC et le PVMC soient utilisés dans les environnements infonuagiques et des fournisseurs de services, respectivement.

Exemple de structure et de libellé de clause

- Les algorithmes de chiffrement dont l'exploitation est autorisée doivent être validés par le Programme de validation des algorithmes cryptographiques (PVAC) et être associés à un certificat figurant dans la liste de validation du PVAC (en anglais seulement).
- Les modules cryptographiques doivent être validés par le Programme de validation des modules cryptographiques (PVMC) et être associés à une certification active du PVMC ainsi qu'à un numéro de certificat figurant dans la liste des modules validés par le PVMC (en anglais seulement).
- Les modules cryptographiques doivent être appliqués et exploités conformément à la stratégie de sécurité des modules cryptographiques figurant dans la liste des modules validés par le PVMC (en anglais seulement), en mode approuvé ou en mode autorisé.

3 Conditions générales d'utilisation

Un fournisseur ou un entrepreneur peut déjà avoir en place des conditions générales d'utilisation pour la vente de ses produits et services. Un grand nombre de clauses recommandées dans cette publication peuvent être appliquées au moyen d'un libellé de clause contractuelle différent (par exemple, en faisant référence aux publications du NIST, plutôt qu'à celles du Centre pour la cybersécurité).

Dans de telles situations, nous recommandons aux organisations de comparer soigneusement les clauses recommandées avec celles présentées par le fournisseur, ainsi qu'avec tous les documents cités par le fournisseur. Ce travail permettra d'aider à assurer des achats de produits et services qui respecteront les exigences en matière de cryptographie de votre organisation. Comme toute situation faisant intervenir des contrats légalement contraignants, nous recommandons de demander des conseils juridiques.

4 Conclusion

La cryptographie offre des moyens importants de protéger les environnements informatiques de votre organisation, que ce soit localement ou dans le nuage. Toutefois, il est important de s'assurer que les produits cryptographiques utilisés par ces systèmes pour protéger vos données sont suffisamment forts et sécurisés. L'utilisation de produits qui respectent les recommandations du Centre pour la cybersécurité en matière de cryptographie, y compris les validations par le PVAC et le PVMC, aidera à assurer efficacement la confidentialité et l'intégrité des données.

Les présents conseils servent à informer les organisations et à les orienter dans l'achat de produits cryptographiques ou l'utilisation de tels produits dans leurs environnements. Comme nous l'avons indiqué, il ne s'agit pas de conseils juridiques.