Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Guide sur le chiffrement des services infonuagiques

ITSP.50.106

Mai 2020

SÉRIE PRATICIENS

Canada

AVANT-PROPOS

Le *Guide sur le chiffrement des services infonuagiques* (ITSP.50.106) est un document NON CLASSIFIÉ publié avec l'autorisation du chef du Centre de la sécurité des télécommunications (CST). Pour en savoir plus ou pour suggérer des modifications, prière de communiquer avec l'équipe des Services à la clientèle du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) :

Centre d'appel du Centre pour la cybersécurité
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le 20 mai 2020.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1	Première version.	20 mai 2020

APERÇU

L'infonuagique pourrait permettre aux organisations d'obtenir, sur demande, des services de technologies de l'information (TI) polyvalents et adaptables selon un mode d'approvisionnement libre-service. Pour tirer avantage de ces possibilités, il est capital de se pencher sur les aspects relatifs à la sécurité et à la protection de la vie privée. Le chiffrement est l'un des principaux éléments qui permettent d'assurer la sécurité et de protéger la vie privée dans un environnement en nuage. Elle joue un rôle capital dans la prestation des services infonuagiques, tels que l'authentification, ainsi que la sécurisation de l'accès aux charges de travail infonuagiques, du stockage des données et des échanges de données.

Les conseils de sécurité contenus dans le présent guide visent à aider votre organisation à comprendre les considérations propres à l'infonuagique qu'il convient de prendre en compte sur le plan du chiffrement. Ce document et ses annexes passent en revue les concepts de la cryptographie et les cas d'utilisation de l'infonuagique, proposent une orientation sur la gestion des clés et donnent des conseils en matière de chiffrement pour les charges de travail des bases de données et les dispositifs d'extrémité.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

1 INTRODUCTION

La forte croissance des services infonuagiques a donné lieu à une constante augmentation du nombre de services de TI mis en œuvre et de données stockées à l'extérieur des limites organisationnelles. Lors de leur migration vers les systèmes infonuagiques, les services de TI et les données sont déployés en fonction de l'infrastructure commune et du modèle de responsabilité, et exposés aux points d'extrémités publics. Les nouveaux services fondés sur l'infonuagique proposent également des fonctionnalités plus décentralisées comme l'Internet des objets, la chaîne de blocs et l'informatique en périphérie. Avant d'adopter l'infonuagique, votre organisation devrait envisager de nouvelles approches et de nouveaux protocoles afin de sécuriser la mise en œuvre et le fonctionnement des services opérationnels, des entités virtuelles et de la protection des données. Les plateformes infonuagiques dépendent largement des mesures cryptographiques pour assurer une prestation sécurisée de tels services.

Bien que le chiffrement joue un rôle essentiel dans la sécurité infonuagique, sa mise en œuvre peut être fort complexe. Les plateformes infonuagiques proposent un grand nombre de services de chiffrement aux clients de services infonuagiques. Il est peut être difficile de comprendre les différents services de chiffrement offerts, les modèles de mise en œuvre, les protocoles, les chiffres et les options de gestion des clés. Par contre, il est important de sélectionner l'approche et la configuration appropriée au déploiement du chiffrement. Une mise en œuvre, une configuration et une gestion inappropriées des services et protocoles de chiffrement pourraient donner lieu à des lacunes graves et à une protection inefficace des données et services en nuage.

Le présent document fournit des conseils sur l'utilisation du chiffrement dans les services fondés sur l'infonuagique. Il fait partie d'une série de documents élaborés par le Centre pour la cybersécurité pour aider à sécuriser les services fondés sur l'infonuagique et il propose aux organisations d'importants facteurs à prendre en compte pour ce qui est d'utiliser le chiffrement comme moyen de protéger efficacement les services et données en nuage.

1.1 POLITIQUES DÉTERMINANTES

Il est impératif d'avoir recours au chiffrement pour protéger les services infonuagiques et s'attaquer aux nombreuses menaces. Cette nécessité est généralement déterminée en fonction des politiques, des directives, des règles, des normes et des lignes directrices applicables à chaque organisation. On peut utiliser les publications mentionnées dans le matériel de référence au moment d'intégrer le chiffrement des services infonuagiques à son programme de sécurité :

- ITSP.40.111, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* [1];[1]
- ITSP.40.062, *Conseils sur la configuration sécurisée des protocoles réseau* [2];
- *Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS)* [3];
- ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [4];
- *Security Guidance for Critical Areas of Focus in Cloud Computing*, version 4.0 [5].

[1] Les numéros entre les crochets renvoient à des ressources qui figurent à la section Contenu complémentaire du présent document.

1.2 ENVIRONNEMENTS CONCERNÉS

Les conseils contenus dans le présent guide s'appliquent aux organisations des secteurs public et privé. Ils peuvent être appliqués aux services fondés sur l'infonuagique, quels que soient les modèles de déploiement en nuage et de services infonuagiques.

1.3 RAPPORT AVEC LA SÉCURITÉ DES TI ET LA GESTION DES RISQUES LIÉS À L'INFONUAGIQUE

L'ITSG-33 [4] propose deux activités de gestion des risques liés à la sécurité des TI que vous pouvez mettre en œuvre dans votre organisation : le niveau du ministère et le niveau du système d'information.

Vous devriez intégrer les activités associées au niveau organisationnel[2] au programme de sécurité de votre organisation pour planifier, gérer, évaluer et améliorer la gestion des risques liés à la sécurité des TI. À ce niveau, le chiffrement des services infonuagiques s'inscrit dans la définition des contrôles de sécurité cryptographique comprise dans le profil de contrôle de sécurité.

Vous devriez intégrer les activités associées au niveau des systèmes d'information[3] au cycle de développement des systèmes. Ces activités comprennent l'ingénierie de sécurité, l'évaluation des menaces et des risques, l'évaluation de la sécurité et l'autorisation des systèmes d'information. L'approche de gestion des risques liés à la sécurité infonuagique du Centre pour la cybersécurité s'aligne sur les activités du niveau des systèmes d'information décrites dans l'ITSG-33 [4]. La figure 1 illustre la relation entre le chiffrement des services infonuagiques et les activités associées au niveau des systèmes d'information, ainsi que les étapes relatives à l'approche de gestion des risques liés à la sécurité infonuagique. Comme l'indique la figure 2, la cinquième étape de l'approche de gestion des risques liés à la sécurité infonuagique appuie la mise en œuvre du chiffrement des services infonuagiques. Vous devriez imposer le recours au chiffrement de données à l'étape 1 (*Effectuer la catégorisation du service*) du processus de gestion des risques liés à la sécurité infonuagique et tout au long des processus d'évaluation des menaces et des risques.

[2] L'annexe 1 de l'ITSG-33 [4] décrit en détail les activités associées au niveau organisationnel.

[3] L'annexe 2 de l'ITSG-33 [4] décrit en détail les activités associées au niveau des systèmes d'information.

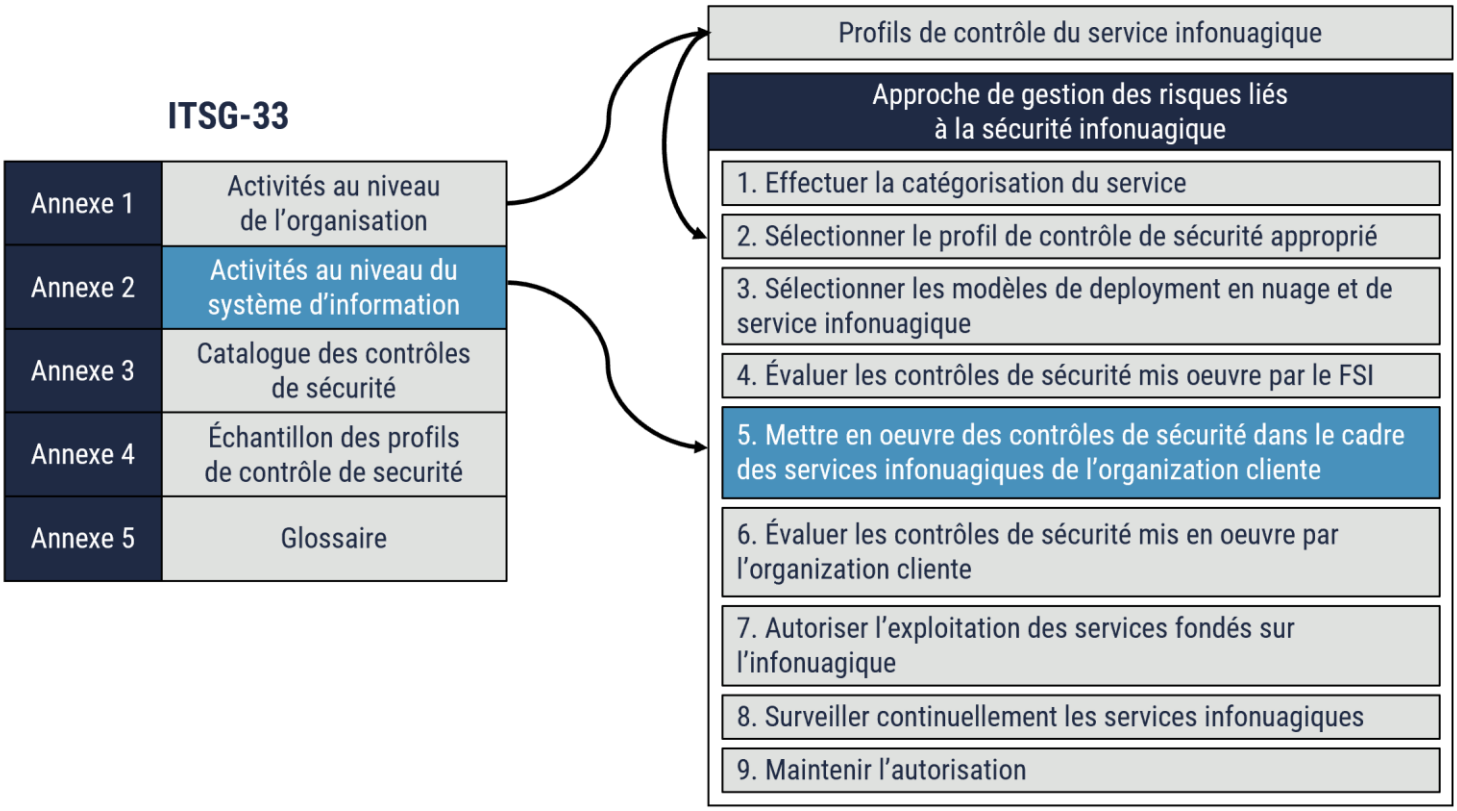

Figure 1 : **Rapport entre le chiffrement des services infonuagiques et la gestion des risques liés à la sécurité des TI**

2 CONTEXTE

2.1 FONCTIONS DE CHIFFREMENT TYPES

L'adoption de l'infonuagique soulèvera des problèmes pour votre organisation sur le plan de la sécurité et du respect de la vie privée. Le fait d'utiliser des ressources partagées réparties dans des emplacements distants et gérées par un tiers n'est pas sans risques. Le chiffrement joue un rôle déterminant dans l'atténuation de ces risques. Il procure les éléments essentiels au soutien des fonctions de confidentialité, d'intégrité, de disponibilité, d'authentification, de non-répudiation et de contrôle de l'accès nécessaires pour sécuriser les plateformes infonuagiques.

2.1.1 CRYPTOGRAPHIE ET CHIFFREMENT

La cryptographie incarne les principes, les techniques et les méthodes de la transformation de données qui visent à en préserver le contenu, ainsi qu'à prévenir les modifications non détectées et une utilisation non autorisée[4]. Le chiffrement est la transformation cryptographique des données en une forme qui masque la signification d'origine des données pour qu'on ne puisse pas les connaître ou les utiliser. Si la transformation est réversible, le processus inverse, qu'on appelle déchiffrement, permettra de restaurer les données chiffrées à leur état initial[5].

2.1.2 CONFIDENTIALITÉ

La confidentialité des données est l'une des principales préoccupations des organisations qui songent à déplacer leurs activités, leurs services et leurs données sur le nuage. Le chiffrement est un des principaux mécanismes utilisés pour assurer la confidentialité des données en transit, des données inactives et, dans certains cas, des données utilisées. Lorsqu'on fait appel au chiffrement, seuls les utilisateurs autorisés peuvent accéder aux données. Voici quelques scénarios types où le chiffrement est utilisé pour assurer la confidentialité des données :

- la protection des mots de passe durant le processus d'authentification;
- la protection des données en transit au moment d'accéder aux charges de travail infonuagiques;
- la protection des données d'authentification et d'autorisation entre les domaines de sécurité (p. ex. dans la fédération des identités);
- la protection de l'information sensible dans l'espace de stockage infonuagique, sur les disques virtuels et dans les bases de données;
- la protection des témoins et des jetons d'assertion;
- la protection des sauvegardes de données;

[4] Définition de « cryptography » (*cryptographie*) tirée du document *Computer Security Resource Centre Glossary* [6] du National Institute of Standards and Technology (NIST).

[5] Définition de « encryption » (*chiffrement*) tirée du document Computer Security Resource Centre Glossary [6] du NIST.

- le nettoyage des supports de stockage infonuagique avant de les réintégrer aux ressources partagées du fournisseur de services infonuagiques (FSI);
- la destruction des données en fin de vie sur les supports de stockage infonuagique;
- la protection des journaux.

2.1.2.1 CHIFFREMENT ET SEGMENTATION EN UNITÉS

Bien que le chiffrement et la segmentation en unités soient des approches souvent utilisées pour assurer la confidentialité des données, ils sont fort différents. En fait, il n'est pas rare que les deux approches soient utilisées concurremment.

Le chiffrement est basé sur des algorithmes mathématiques qui sont combinés à une clé secrète afin de convertir des données en texte clair en texte chiffré. L'inconvénient de cette méthode est que la compromission du matériel de chiffrement peut donner lieu à une divulgation non autorisée des données.

La segmentation en unités repose sur un processus qui consiste à remplacer certains éléments des données sensibles par des équivalents non sensibles, appelés jetons, qui n'ont aucune signification ou valeur extrinsèque ou exploitable[6]. Les jetons et les valeurs sensibles en question sont stockés dans une base de données de jetons par le système de segmentation en unités, séparément des applications en nuage. Les valeurs initiales ne sont jamais stockées avec les applications, seulement les jetons. Comme l'application en nuage accède aux jetons seulement, et non aux valeurs sensibles, elle ne fait généralement pas l'objet des vérifications réglementaires. Cette approche génère des économies considérables pour les organisations qui sont sujettes à des réglementations telles que les *Normes de sécurité sur les données de l'industrie des cartes de paiement* (PCI DSS pour *Payment Card Industry Data Security Standard*). La compromission des bases de données de segmentation des unités peut donner lieu à une divulgation non autorisée des données.

Aucune pratique exemplaire n'a encore été mise en place en ce qui a trait à la segmentation en unités dans un environnement en nuage et aucun conseil n'a été formulé à ce sujet. Les clients de services infonuagiques qui veulent obtenir de plus amples renseignements sur l'utilisation sécurisée de la segmentation en unités devraient se référer aux directives émises par le Conseil des normes de sécurité PCI.

2.1.3 INTÉGRITÉ

Pour tirer avantage des capacités de l'infonuagique, votre organisation doit est en mesure d'assurer la confidentialité de l'information. Cela dit, l'intégrité de l'information peut être tout aussi importante, sinon plus. Votre organisation doit s'assurer que les protocoles de transmission tiennent compte à la fois de la confidentialité et de l'intégrité des données. Sur des plateformes infonuagiques, les données passent par une infrastructure réseau qui échappe au contrôle des clients du service infonuagique. Cela comprend les flux de données entre les environnements locaux et en nuage, ainsi que le flux de données entre les services infonuagiques. Les clients du service infonuagique n'ont également aucun contrôle sur l'infrastructure de stockage. Des modifications peuvent être apportées aux données lorsqu'elles sont en transit ou en

[6] Définition de « tokenization » (*segmentation en unités*) tirée de Wikipédia. https://en.wikipedia.org/wiki/Tokenization_(data_security) (en anglais seulement).

stockage et votre organisation pourrait ne pas être en mesure de déterminer si elles ont été modifiées. Ces modifications pourraient être le résultat d'une dysfonction des systèmes ou des logiciels, d'une erreur humaine ou de changements non autorisés effectués par des auteurs de menace. Le chiffrement permet de détecter toute modification non autorisée des données alors qu'elles sont en transit ou en stockage.

Le chiffrement fournit la fonction d'intégrité des données nécessaire aux certificats numériques et aux cas d'utilisation mentionnés à la section 2.1.1. La confidentialité et l'intégrité font appel aux différents mécanismes de chiffrement pour répondre à leurs objectifs de sécurité. L'intégrité est généralement réalisée à l'aide d'un hachage cryptographique et de signatures numériques.

2.1.4 AUTHENTIFICATION

Le chiffrement joue un rôle important dans l'authentification. Il prend en charge la fonction d'authentification à plusieurs niveaux de l'infonuagique, ce qui comprend ce qui suit :

- la signature des certificats;
- le hachage des mots de passe;
- l'établissement de l'identité d'un site Web;
- l'authentification des interfaces de programmation d'applications (API pour *Application Program Interfaces*) au moyen de clés cryptographiques;
- la protection des jetons d'assertion lorsqu'on fait appel à la fédération des identités.

Les clients de services infonuagiques doivent s'assurer que les fonctions de chiffrement et les configurations utilisées pour prendre en charge l'authentification sur la plateforme infonuagique du FSI, ainsi que la charge de travail infonuagique, soient suffisamment robustes. L'utilisation de protocoles, de fonctions de hachage ou de chiffres moins sécurisés effrite la confiance accordée à l'identité des ressources, des applications et des utilisateurs, et peut avoir de graves répercussions sur la sécurité du déploiement en nuage[7].

2.1.5 NON-RÉPUDIATION

Le concept de non-répudiation permet d'établir qu'une transaction donnée a bien été effectuée par un utilisateur ou un service infonuagique en particulier. La mise en œuvre de la non-répudiation est généralement réalisée au moyen de signatures numériques et de journaux de vérification. Par exemple, l'infonuagique repose souvent sur la fédération des identités. Selon cette approche, un vérificateur émet une assertion afin de valider l'identité d'un demandeur pour une partie de confiance (PC). Il convient de protéger de telles assertions contre toute répudiation par le vérificateur, ce qui est souvent effectué au moyen d'une signature numérique.

[7] Pour une description détaillée des facteurs de la cryptographie à considérer pour la fonction d'authentification, prière de consulter la version 3 de l'ITSP.30.031, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* [7].

2.2 DONNÉES EN TRANSIT, INACTIVES ET UTILISÉES

2.2.1 DONNÉES EN TRANSIT

Le transit des flux de données à destination, en provenance et à l'intérieur d'environnements infonuagiques passe par une infrastructure réseau hors du contrôle des clients de services infonuagiques. Des auteurs de menace pourraient intercepter ces données et en compromettre la confidentialité et l'intégrité. Les organisations devraient veiller à ce que les données en transit soient chiffrées de manière à sécuriser les communications à destination et en provenance des environnements infonuagiques.

Les organisations contrôlent le périmètre de l'infrastructure en tant que service (IaaS pour *Infrastructure as a Service*), mais les communications comporteront sans doute des échanges d'information avec des services infonuagiques à l'extérieur du périmètre. Elles risquent toutefois de ne pas connaître l'emplacement des instances qui contribuent au transfert de données. Par exemple, les instances de machines virtuelles (VM pour *Virtual* Machine) d'un client se trouvent peut-être dans différents centres de données du FSI, et les communications peuvent être transmises sur une infrastructure réseau qui ne relève pas du contrôle du client et du FSI. Il convient donc de chiffrer les communications de données dans un environnement infonuagique dès qu'il s'agit d'information sensible.

Bien que le chiffrement côté client puisse être utilisé avant le transfert de données, on recommande de faire appel au protocole HTTPS (Hypertext Transfer Protocol Secure) pour le chiffrement de bout en bout afin d'assurer l'intégrité des données[8]. Les organisations devraient :

- configurer les services infonuagiques de manière à autoriser uniquement l'utilisation du protocole HTTPS pour accéder aux services de stockage infonuagique et aux API;
- désactiver et interdire les algorithmes de chiffrement faibles;
- autoriser les autres protocoles réseau chiffrés en fonction d'applications particulières (p. ex. le protocole de bloc de messages de serveur [SMB pour *Server Message Block*] pour l'accès au stockage de fichiers).

2.2.2 DONNÉES INACTIVES

Le chiffrement des données inactives permet de les protéger lorsqu'elles sont stockées sur des supports physiques ou virtuels, en plus d'en prévenir la divulgation ou la modification non autorisée, et de s'inscrire dans l'approche globale de défense en profondeur. Les clients et les FSI auront peut-être mis en œuvre des contrôles à divers niveaux afin de protéger les données, mais le chiffrement des données inactives offre une protection additionnelle advenant l'échec des autres mesures de sécurité.

Il est fortement recommandé aux organisations de prévoir le chiffrement des données inactives dans leur stratégie de défense en profondeur. Votre organisation devrait mettre à jour ses stratégies de sécurité de manière à tenir compte des exigences liées au chiffrement des données inactives et à déterminer les classes de données qui doivent être chiffrées sur

[8] Pour de plus amples renseignements sur les facteurs de la cryptographie à considérer pour l'utilisation du protocole HTTPS, prière de consulter l'ITSP.40.062 [2].

le stockage en nuage. Votre organisation devrait envisager de chiffrer les données inactives pour protéger la confidentialité et l'intégrité des données, des images de VM, des instantanés de VM, des vidages de mémoire, des applications, des sauvegardes et d'autres informations et services importants.

Dans un environnement infonuagique multilocataire, le chiffrement des données inactives peut servir à isoler davantage les données d'une organisation de celles des autres locataires et du personnel du FSI. Les organisations pourraient devoir chiffrer les données inactives pour se conformer aux lois sur la protection de la vie privée, ainsi qu'aux règlements de l'industrie et du gouvernement. Il pourrait même être obligatoire de se conformer à certaines exigences réglementaires et de conformité. Par ailleurs, le chiffrement des données inactives permet à votre organisation de nettoyer les données avant que les ressources de stockage ne soient retournées aux ressources partagées du FSI (voir la section 3.4 pour plus de renseignements sur le cryptodéchiquetage).

Les FSI activent souvent par défaut le chiffrement du stockage d'objets et de fichiers, mais la configuration par défaut peut changer au fil du temps. Les organisations devraient avoir recours aux configurations de sécurité de base et à la surveillance continue pour veiller à l'application du chiffrement des données inactives. Les approches de chiffrement des données présentées à la figure 2 protègent la confidentialité et l'intégrité des données contre l'accès non autorisé aux supports physiques. Elles ne fourniront cependant pas toutes une protection efficace contre la compromission de plateformes, de systèmes d'exploitation ou d'applications. Les organisations devraient tenir compte d'un certain nombre de facteurs avant de choisir une stratégie de chiffrement des données inactives, notamment le type de stockage, l'environnement où se trouvent les données (plateforme, système d'exploitation, application), la quantité d'informations à protéger et les menaces devant être atténuées. Par exemple, les options de chiffrement du modèle de plateforme en tant que service (PaaS pour *Platform as a Service*) pourraient varier d'une plateforme à l'autre, tandis que les fournisseurs de modèles de logiciel en tant que service (SaaS pour *Software as a Service*) pourraient utiliser n'importe quelle option de la figure 2.

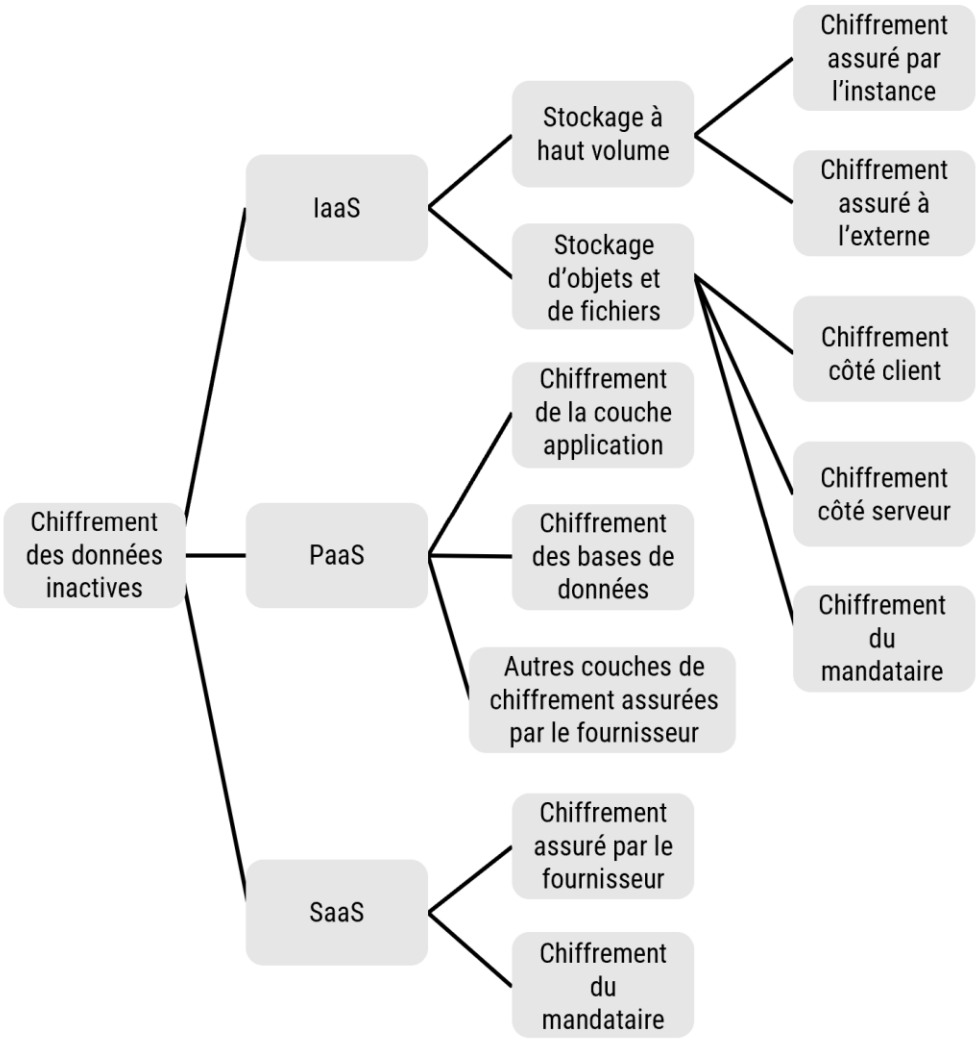

Figure 2 : **Approches de chiffrement**[9]

2.2.3 DONNÉES UTILISÉES

Les données utilisées font généralement référence aux données étant en cours de traitement par le processeur ou étant stockées dans la mémoire vive d'un ordinateur. Bien qu'il soit possible de chiffrer les données alors qu'elles sont inactives et en transit, il est impératif de les déchiffrer avant qu'elles soient traitées par les charges de travail infonuagique. Il existe des solutions tierces, mais comme leurs mises en œuvre n'ont pas été validées ou évaluées, elles pourraient ne pas offrir le niveau d'assurance nécessaire. Les approches adoptées pour le chiffrement des données utilisées sont toujours considérées comme étant de nouvelles technologies. Les clients de services infonuagiques doivent analyser avec soin les

[9] Les options de chiffrement sont fondées sur la publication du Cloud Security Alliance (CSA) intitulée *Security Guidance for Critical Areas of Focus in Cloud Computing*, version 4 [5].

possibles avantages (p. ex., prévenir la visibilité des données), les préoccupations (p. ex., les données pourraient contenir des éléments associés à la propriété intellectuelle) et les risques (p. ex., les données pourraient contenir des certificats numériques) associés au chiffrement des données utilisées avant de se procurer, de déployer ou d'utiliser de telles solutions.

Comme le traitement des données utilisées est généralement effectué à partir d'information non chiffrée, ce qui pourrait comprendre le matériel de chiffrement dans certains cas, les clients de services infonuagiques devraient veiller à ce que les instantanés de VM, les vidages de mémoire et les sauvegardes soient adéquatement protégés lorsque non utilisés. En l'absence d'une protection matérielle suffisante dans le nuage privé interne, le chiffrement demeure la meilleure façon de protéger les instantanés de VM. Le chiffrement des instantanés de VM peut être réalisé directement à travers les services offerts par le fournisseur infonuagique ou encore par ceux de fournisseurs tiers.

2.3 CONTRÔLES DE SÉCURITÉ LIÉS AU CHIFFREMENT INFONUAGIQUE

Les profils de contrôle de la sécurité infonuagique du Centre pour la cybersécurité mentionnés dans l'ITSP.50.103, *Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique* [7], font état de plusieurs contrôles de sécurité associés à l'utilisation du chiffrement dans des déploiements en nuage. Les contrôles de sécurité connexes sont indiqués dans le tableau 1 ci-dessous.

Tableau 1 : **Contrôles de sécurité liés au chiffrement infonuagique**

ID du contrôle de sécurité	Titre
AU-2	Événements vérifiables
AU-12	Génération d'enregistrements de vérification
IA-3	Identification et authentification des dispositifs
IA-3(1)	Identification et authentification des dispositifs | Authentification bidirectionnelle cryptographique
IA-5(2)	Gestion des authentifiants | Authentification fondée sur l'ICP
IA-5(6)	Gestion des authentifiants | Protection des authentifiants
IA-5(7)	Gestion des authentifiants | Aucun authentifiant statique intégré non chiffré
IA-7	Authentification des modules cryptographiques
SC-8(1)	Confidentialité et intégrité des transmissions
SC-12	Établissement et gestion des clés cryptographiques
SC-12(1)	Établissement et gestion des clés cryptographiques | Disponibilité
SC-12(2)	Établissement et gestion des clés cryptographiques | Clés symétriques
SC-12(3)	Établissement et gestion des clés cryptographiques | Clés asymétriques
SC-13	Protection cryptographique
SC-17	Certificats d'infrastructure à clé publique

ID du contrôle de sécurité	Titre
SC-23	Authenticité des sessions
SC-28(1)	Protection de l'information inactive | Protection cryptographique
SI-7(1)	Intégrité des logiciels, des micrologiciels et de l'information | Contrôles d'intégrité

3 CONSEILS EN MATIÈRE DE CHIFFREMENT

3.1 ALGORITHMES DE CHIFFREMENT ET PROTOCOLES RECOMMANDÉS

L'efficacité du chiffrement de services infonuagiques repose sur la robustesse des clés, des algorithmes, des chiffres et des protocoles utilisés tout au long du cycle de vie de la gestion des clés et de leur utilisation. L'ITSP.40.111 [1] définit les algorithmes cryptographiques approuvés ainsi que les méthodes d'utilisation appropriées pour protéger la confidentialité de l'information PROTÉGÉ A et PROTÉGÉ B ainsi que l'intégrité de l'information associée à un niveau de préjudice moyen ou inférieur[10]. Les clients devraient s'assurer que leur modèle de déploiement en nuage respecte les conseils formulés dans l'ITSP.40.111 [1]. Les clients de services infonuagiques doivent évaluer les contrôles mis en place par le FSI pour en assurer la conformité avec les conseils formulés[11]. Votre organisation devrait évaluer et définir soigneusement les paramètres de configuration des services infonuagiques connexes.

Les clients de services infonuagiques doivent également configurer les protocoles réseau de façon sécurisée. L'ITSP.40.062 [2] traite des sujets suivants :

- les mesures permettant de configurer les protocoles réseau de façon sécurisée afin de protéger la confidentialité et l'intégrité de l'information associée à un niveau de préjudice moyen ou inférieur;
- les algorithmes recommandés pour ces protocoles réseau;
- les normes de référence et les publications du National Institute of Standards and Technology (NIST) qui offrent de l'information supplémentaire sur ces protocoles réseau.

L'application des conseils formulés dans ces deux publications permettra à votre organisation de veiller à ce que ses déploiements en nuage et son information soient protégés au moyen d'algorithmes de chiffrement et de protocoles qui ont fait l'objet d'analyses, dont la conformité aux normes reconnues est vérifiée par des organismes faisant autorité dans le cadre de tests rigoureux, et dont la robustesse est évaluée au fil du temps. Si des lacunes sont relevées dans les protocoles et les algorithmes, les organismes gouvernementaux chargés de la sécurité et les organismes de normalisation mettent à jour leurs directives de manière à inclure des versions plus sécurisées et des recommandations sur leur mise en œuvre.

Les attaques par force brute qui touchent le chiffrement ne sont pas des menaces dont il faut tenir compte si on fait appel à des algorithmes de chiffrement approuvés par le Centre pour la cybersécurité. Par contre, les menaces suivantes doivent être identifiées et atténuées dans le cadre du processus de gestion des risques à la sécurité :

- attaques opportunistes contre les défauts de mise en œuvre;
- intégration non sécurisée de la cryptographie dans les applications et les protocoles;

---

[10] Par catégorisation de la sécurité, on entend le processus permettant d'identifier le possible préjudice lié à la compromission des processus opérationnels et de l'information connexe. Se reporter à l'ITSP.50.103, *Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique* [8].

[11] L'ITSP.50.105, *Guide sur l'évaluation et l'autorisation de la sécurité infonuagique* [9], décrit l'approche à adopter concernant l'évaluation des contrôles mis en place par les FSI.

- lacunes dans la conception, la gestion et le fonctionnement des systèmes de gestion des clés;
- coercition ou corruption du personnel de confiance qui a accès au matériel de chiffrement cryptographique.

3.2 ALGORITHMES DE CHIFFREMENT ET PROTOCOLES EXCLUSIFS

Il convient d'éviter les services infonuagiques qui emploient des algorithmes et protocoles exclusifs et s'assurer que de tels algorithmes et protocoles ne sont pas utilisés dans le cadre de votre évaluation des contrôles de sécurité du FSI. Votre organisation devrait avoir recours à des algorithmes de chiffrement et des protocoles recommandés par le CST. Vous devriez également vous servir des options de configuration des services infonuagiques pour désactiver et interdire l'utilisation du chiffrement propriétaire.

Par chiffrement propriétaire, on entend l'utilisation d'algorithmes, de chiffres et de protocoles qui sont gardés secrets. Les fournisseurs peuvent faire appel au chiffrement propriétaire pour différentes raisons. Parmi les raisons pour lesquelles on utilise souvent ce type de chiffrement, on retrouve la nécessité d'avoir recours à des protocoles légers, d'améliorer les performances et d'améliorer la sécurité.

En règle générale, les fournisseurs diffusent publiquement les détails liés à la mise en œuvre des algorithmes de chiffrement et des protocoles propriétaires, ou les soumettent aux organismes responsables aux fins d'évaluation. Comme ces détails ne font pas l'objet d'une évaluation indépendante, les fournisseurs ne peuvent tirer avantage des commentaires formulés par la communauté scientifique, les organismes de normalisation et la collectivité internationale d'experts en sécurité des TI. En l'absence d'examen indépendant, les clients de services infonuagiques ne peuvent avoir la certitude que les protocoles mis en place offrent la robustesse requise, ne présentent aucune lacune et ne contiennent aucune porte dérobée. Les auteurs de menace peuvent exploiter ces lacunes dont le fournisseur peut ne pas être au courant afin de compromettre la confidentialité, l'intégrité et la disponibilité des services fondés sur l'infonuagique et des données.

3.3 OPTIONS DE GESTION DE CLÉS POUR LES SERVICES INFONUAGIQUES

La gestion des clés est un élément important du chiffrement des services infonuagiques. Il s'agit d'une initiative complexe qu'on aurait tort de sous-estimer. La gestion des clés peut être effectuée par le FSI ou le client. Les activités de gestion du cycle de vie des clés comprennent la génération, la distribution, l'entreposage, la révocation, la récupération et la destruction des clés de chiffrement. Un processus inefficace de gestion des clés risque de compromettre la confidentialité, l'intégrité et la disponibilité des données. Les clients de services infonuagiques peuvent consulter le document *Special Publication 800-57 Recommendation for Key Management, Part 1: General (Revision 4)* [10] du NIST pour des conseils sur l'élaboration d'un programme de gestion des clés efficace.

Avant d'évaluer les options de gestion des clés et de mettre en place une stratégie de gestion des clés pour les déploiements en nuage, les clients de services infonuagiques devraient considérer les points suivants :

- **Exigences et implications réglementaires :** cela peut comprendre la nécessité que la solution de gestion des clés proposée par le FSI réponde aux exigences de conformité des normes PCI DSS[12] et respecte les règlements sur la protection des renseignements personnels;
- **Exigences et implications relatives à la souveraineté et à la résidence des données :** les données des clients de services infonuagiques peuvent être assujetties aux lois d'autres pays, peu importe où se trouvent les données. Dans de telles situations, un FSI menant des activités à l'étranger pourrait être tenu de se conformer à une ordonnance de la cour, à un mandat ou à une citation à comparaître émis par un organisme étranger chargé de l'application de la loi qui cherche à obtenir les données de clients de services infonuagiques[13]. Si les données sont chiffrées avec des clés gérées par le FSI, ce dernier pourrait être dans l'obligation de se conformer à un ordre légal et donner accès aux clés de chiffrement de ses clients et aux données de votre organisation;
- **Exigences relatives aux protocoles, aux interfaces et aux API (p. ex. protocole d'interopérabilité de gestion des clés [KMIP] pour *Key Management Interoperability Protocol*) :** les clients de services infonuagiques peuvent avoir recours à des solutions de TI qui utilisent le KMIP pour gérer une clé d'application susceptible de ne pas prendre en charge l'API fournie par le FSI aux fins du service de gestion des clés (SGC);
- **Modèle de service infonuagique :** certaines solutions infonuagiques de gestion des clés ne sont compatibles qu'avec les solutions IaaS, alors que d'autres sont compatibles avec tous les modèles de service.

Le choix d'une solution de gestion des clés adéquate varie d'une organisation à l'autre et repose sur les critères qui sont les plus importants pour votre organisation. Trois approches peuvent être adoptées en ce qui concerne la gestion des clés dans un service infonuagique :

- les clés sont contrôlées et gérées par le FSI;
- les clés sont contrôlées par le FSI et gérées par le client du service infonuagique;
- les clés sont contrôlées et gérées par le client du service infonuagique.

Si les clés sont contrôlées par le FSI, ce dernier peut y avoir accès, même si elles sont gérées par le client du service infonuagique. Par exemple, il est pratique courante pour les FSI de fournir un système de gestion des clés (SGC) à leurs clients. Dans un tel cas, le FSI contrôle le SGC et peut potentiellement accéder aux clés pour répondre aux demandes d'un organisme étranger chargé de l'application de la loi.

[12] Les organisations devant se conformer aux nomes du PCI devraient consulter le document intitulé *PCI DSS Cloud Computing Guidelines* [11].

[13] Se reporter à la publication du Secrétariat du Conseil du Trésor intitulée *Gouvernement du Canada, Livre blanc : Souveraineté des données et nuage public* [12].

Les clients de services infonuagiques peuvent utiliser plusieurs modèles de gestion des clés. Votre organisation peut décider de sécuriser la majeure partie de ces données au moyen de clés contrôlées par le FSI, puis d'utiliser les clés qu'elle gère et contrôle pour protéger les données très sensibles.

3.3.1 CLÉS CONTRÔLÉES ET GÉRÉES PAR UN FSI

On déconseille aux organisations tenues de remplir des exigences réglementaires et de conformité rigoureuses de mettre en place ce modèle de gestion des clés, puisqu'elles risquent de ne pas se conformer aux exigences imposées par les organes d'examen applicables.

Selon ce modèle, le FSI est responsable de tous les aspects de la gestion des clés. Ces aspects comprennent la sécurité physique, l'infrastructure et les logiciels de gestion des clés, le stockage de clés sécurisé, l'isolement par rapport aux autres locataires, et la mise en œuvre des fonctions de gestion des clés (p. ex. le contrôle d'accès et le chiffrement). Le FSI est également responsable de la mise en place du processus de gestion des clés. En règle générale, votre organisation configure les options de protection de données (p. ex. le stockage, le disque virtuel et le chiffrement des bases de données) au moment de s'inscrire à un service infonuagique, puis le FSI s'occupe de la gestion des clés.

Dans le cas de certains modèles SaaS et PaaS, ce modèle de gestion des clés est la seule option offerte. Par exemple, une solution PaaS avec base de données peut offrir des paramètres de configuration afin de chiffrer les données inactives et en transit, mais n'offrir aux clients de services infonuagiques aucun mécanisme permettant d'assurer la gestion des clés. Les clients de services infonuagiques qui sont tenus de contrôler ou de gérer les clés devraient s'assurer que ces options sont offertes par le FSI.

Ce modèle de gestion des clés est le plus facile à mettre en œuvre. Il n'exige aucune configuration additionnelle et le client du service infonuagique n'a pas à planifier les fonctionnalités, la performance ou l'extensibilité de la solution. Par contre, le client du service infonuagique n'a aucun contrôle sur la façon dont les clés sont stockées et où elles sont stockées, et ne peut pas consulter les journaux de vérification associés à l'accès aux clés et à leurs activités.

3.3.2 CLÉS CONTRÔLÉES PAR LE FSI ET GÉRÉES PAR LE CLIENT DU SERVICE INFONUAGIQUE

Selon ce modèle, les clients s'inscrivent au SGC du FSI, un service faisant généralement partie des services offerts. Le SGC du FSI est mis en œuvre en tant que service multilocataire. L'accès aux clés est généralement fourni depuis un portail Web, une interface de ligne de commande ou une API. Le SGC d'un FSI est intégré au système de gestion des identités et de l'accès et à la fonction de vérification de ce dernier. Il permet aux clients du service infonuagique de gérer et surveiller l'accès au matériel de chiffrement.

Un SGC géré par le FSI est un moyen pratique et peu coûteux de gérer les clés, les secrets et les certificats de votre organisation. Selon ce modèle, le client du service infonuagique contrôle l'emplacement géographique où seront créées les clés et peut se conformer aux exigences liées à la résidence des données. Il importe de souligner que les services associés au SGC et au module de sécurité matériel (HSM pour *Hardware Security Module*) offerts par certains FSI ne sont pas hébergés au Canada.

Ce modèle de gestion des clés repose sur la responsabilité conjointe de votre organisation et du FSI. Ce dernier est responsable de la sécurité physique, de l'infrastructure de gestion des clés, du stockage sécurisé des clés, de l'isolement par rapport aux autres locataires et de la mise en œuvre des fonctions de gestion des clés (p. ex. le contrôle d'accès et le chiffrement). Votre organisation est responsable de la mise en œuvre du processus de gestion des clés et de la configuration des services infonuagiques et des applications à utiliser afin que le SGC puisse accéder aux clés nécessaires. Ce modèle de gestion des clés est le plus difficile à mettre en œuvre. Si votre organisation décide d'adopter ce modèle, elle devra faire ce qui suit :

- élaborer des processus de gestion des clés bien conçus, documentés et mis à l'essai;
- activer les journaux de vérification fournis par le FSI pour tous les accès aux clés et toutes les actions qui y sont associées;
- restreindre les opérations liées aux clés selon le principe du droit d'accès minimal;
- utiliser le SGC du FSI pour simplifier ses processus de gestion des clés[14].

Ce modèle de gestion des clés offre un meilleur contrôle du cycle de vie de la gestion des clés. Par exemple, si vous pensez avoir été victime d'un accès non autorisé ou d'une divulgation d'information, vous pouvez révoquer les clés afin de mettre fin à l'exfiltration de données, car vous êtes responsable de la gestion de ces clés.

Selon ce modèle de gestion des clés, le FSI contrôle le SGC et a potentiellement accès aux clés gérées par votre organisation. S'il peut accéder à la fois aux clés et aux données, le FSI a la possibilité de déchiffrer les données. Pour éviter qu'une telle situation se produise, votre organisation peut examiner et vérifier les processus et les contrôles mis en place par le FSI. Les clés et les données pourraient toutefois être exposées si le FSI doit se conformer à une ordonnance de la cour, à un mandat ou à une citation à comparaître émis par un organisme étranger chargé de l'application de la loi.

Ce modèle de gestion des clés peut être appliqué à tous les modèles de service et de déploiement. Il n'est toutefois pas pris en charge par toutes les solutions PaaS ou SaaS.

3.3.2.1 SERVICE BRING YOUR OWN KEYS (BYOK)

Le service Bring your own key (BYOK) permet aux clients de services infonuagiques de générer leurs propres clés au moyen des services de génération des clés offerts sur place ou par un fournisseur externe. Les clés générées sont généralement stockées sur un HSM qui se trouve sur le site et qui est contrôlé par le client du service infonuagique. Une fois générées, les clés peuvent être exportées en toute sécurité dans un SGC en nuage. Le SGC peut protéger les clés avec un HSM.

En mettant en œuvre les politiques relatives à l'utilisation des clés, votre organisation peut empêcher un FSI d'exporter les clés de chiffrement du client et de les utiliser à l'extérieur du SGC en nuage. Un FSI peut toutefois accéder aux clés que votre organisation a exportées sur le SGC en nuage. Bien que le service BYOK permette à votre organisation de conserver le contrôle des clés qui sont stockées sur le site, le FSI pourra y accéder une fois que vous les aurez exportées vers un SGC en

[14] Le SGC d'un FSI pourrait ne pas être accessible dans tous les pays. Les clients de services infonuagiques qui ont des exigences concernant la résidence des données devraient s'assurer que le SGC est accessible et hébergé au Canada.

nuage. À titre d'exemple, le FSI devra avoir accès aux clés pour que son service de stockage puisse chiffrer et déchiffrer les données.

Les services BYOK proposent les avantages suivants par rapport aux clés générées par le FSI :

- contrôle total de la génération des clés;
- meilleur contrôle du cycle de vie des clés;
- capacité de révoquer les clés et d'empêcher quiconque de déchiffrer les données qui sont chiffrées avec la clé;
- protection contre les blocages des fournisseurs, car le client conserve une copie de la clé et peut facilement migrer ses services à un autre fournisseur.

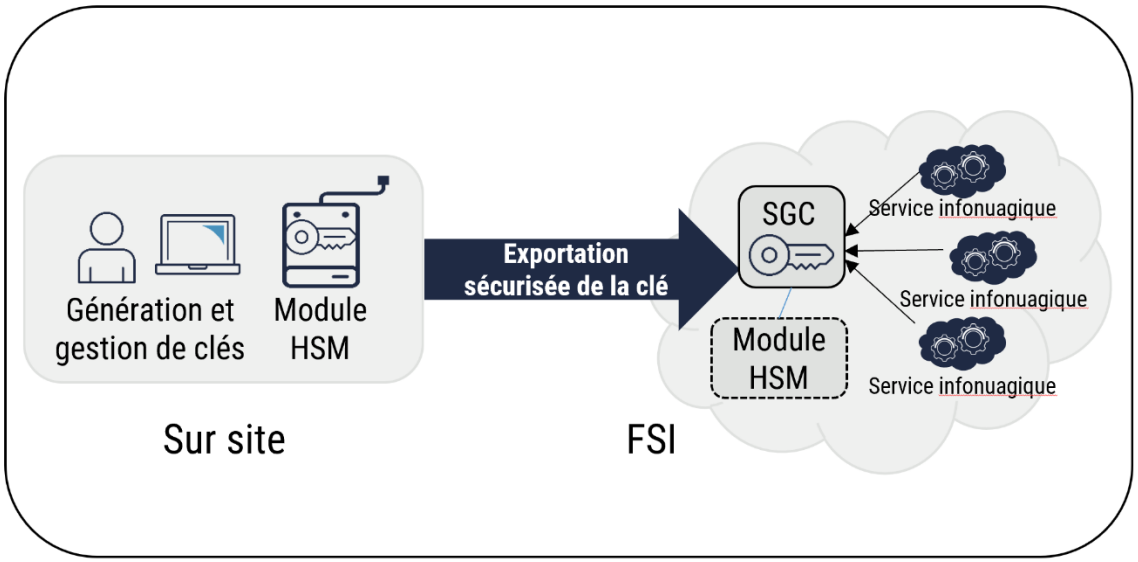

Figure 3 : **Concept du service BYOK**

3.3.3 CLÉS CONTRÔLÉES ET GÉRÉES PAR LE CLIENT DU SERVICE INFONUAGIQUE

Si votre organisation doit répondre à des exigences de sécurité ou est assujettie à une réglementation très stricte, vous pourriez avoir à stocker les données sur le nuage tout en veillant à ce que le FSI ne puisse pas les déchiffrer. Dans de tels scénarios, il incombe à votre organisation de contrôler et de gérer les clés. Parmi les approches prenant en charge ce cas d'utilisation de gestion des clés, on retrouve :

- l'abonnement à des services HSM infonuagiques dédiés;
- l'utilisation de passerelles tierces dédiées ou d'un courtier de sécurité d'accès au nuage (CASB pour *Cloud Access Security Broker*);
- l'utilisation d'un SGC tiers.

Ce modèle de gestion des clés offre les avantages suivants :

- permet à votre organisation de contrôler l'identité de ceux qui ont accès à vos données;
- respecte les exigences relatives à la résidence des données;
- évite de dépendre totalement des produits d'un fournisseur;
- permet la destruction contrôlée des données, puisque le client détruit les clés de chiffrement.

Un des inconvénients de cette approche à la gestion des clés est que certains services infonuagiques, comme l'indexation, la recherche et la prévention de la perte de données, sont inefficaces en ce qui a trait aux données chiffrées. Votre organisation est toujours assujettie aux ordonnances de la cour et aux citations à comparaître et il pourrait être nécessaire de fournir les données dans de telles situations.

3.3.3.1 HSM EN NUAGE DÉDIÉ

Un HSM est un dispositif matériel qui sauvegarde et gère les clés numériques pour assurer une authentification forte. Un HSM permet également de traiter le chiffrement. Le matériel de chiffrement est stocké dans des modules matériels inviolables et les applications doivent être authentifiées et autorisées avant d'accéder au matériel de chiffrement. Celui-ci ne quitte jamais la limite de protection du HSM.

Les services HSM en nuage fournissent généralement un HSM dédié aux clients du service infonuagique[15]. Le client contrôle et gère toutes les activités menées sur ce HSM. Dans la plupart des cas, les HSM en nuage se limitent au mode IaaS, ce qui signifie que les clients de services infonuagiques ne peuvent pas utiliser le matériel de chiffrement à partir des HSM en nuage s'ils optent pour une solution PaaS et SaaS.

Certains FSI offrent aux clients la capacité d'autoriser le SGC à accéder à leur HSM dédié[16]. Cette approche a pour avantage de permettre aux clients de services infonuagiques d'utiliser des solutions PaaS et SaaS avec un HSM dédié pour assurer le stockage des clés. Cette approche offre aux clients de services infonuagiques la polyvalence nécessaire pour utiliser des solutions PaaS et SaaS tout en étant fort similaire avec le service BYOK. Les FSI menant des activités à l'étranger peuvent accéder aux clés afin de se conformer à une demande d'un organisme étranger chargé de l'application de la loi qui cherche à obtenir les données de clients de services infonuagiques. Par conséquent, si votre organisation doit maintenir le contrôle des clés, il est préférable d'éviter que le SGC du FSI puisse accéder à votre HSM dédié en nuage.

[15] Certains HSM dédiés sont hébergés sur des dispositifs physiques partagés avec d'autres locataires.

[16] Les HSM d'un FSI pourraient ne pas être accessibles dans tous les pays. Les clients de services infonuagiques qui ont des exigences concernant la résidence des données devraient s'assurer que le HSM du FSI est accessible et hébergé au Canada.

3.3.3.2 PASSERELLES DE CHIFFREMENT EN NUAGE (CEG) ET CASB

Les passerelles de chiffrement en nuage (CEG pour *Cloud Encryption Gateway*) et les CASB font office de mandataires entre les réseaux locaux du client et les services infonuagiques. Ils sont généralement déployés localement. Les CEG et CASB peuvent intercepter les données sensibles et utiliser des techniques de segmentation en unités et de chiffrement pour dissimuler l'information sensible avant qu'elle soit transmise au nuage aux fins de stockage ou de traitement. Les CEG et CASB peuvent être intégrés aux services infonuagiques au moyen d'API sécurisées. Cette intégration permet aux clients de services infonuagiques de contrôler et de gérer les clés, le chiffrement et les stratégies de protection de l'information. Les données sensibles sont dissimulées avant d'être acheminées aux services infonuagiques.

Vous devez vous assurer que les exigences de votre organisation en matière de résidence de données sont satisfaites. Contrairement aux autres approches, votre organisation pourrait être appelée à divulguer de l'information sensible afin de se conformer à des ordonnances de la cour ou des citations à comparaître. Votre organisation devrait évaluer attentivement ses exigences avant d'opter pour une solution CEG. Cette approche repose sur ce qui suit :

- la structure du réseau;
- les emplacements;
- la possibilité d'intégrer les solutions de tiers;
- le volume de données.

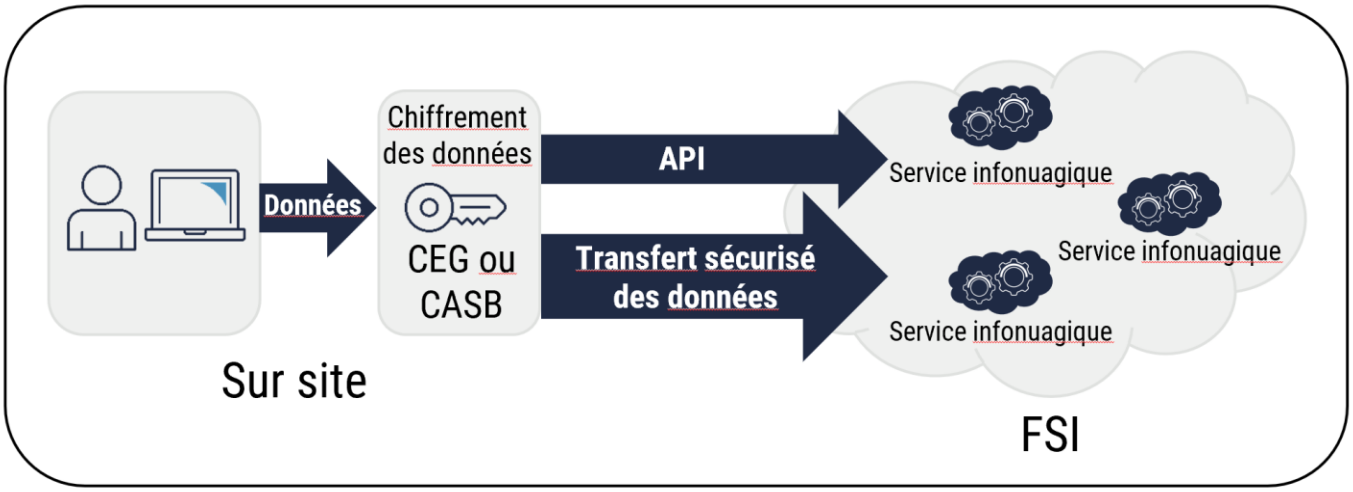

Figure 4 : **Chiffrement de données au moyen de CEG ou d'un CASB**

3.3.3.3 SERVICES DE GESTION DE CLÉS D'UN TIERS

Le fait que les fournisseurs de services aient accès aux clés et aux données pourrait donner lieu à un accès non autorisé. Une façon de prévenir les accès non autorisés est de contrôler les données et les clés séparément. On peut faire appel au service de gestion des clés d'un tiers pour séparer la fonction de contrôle du matériel de chiffrement et celle des données. Il est ainsi possible de contrôler et de surveiller les accès au matériel de chiffrement et d'utiliser le service de gestion des clés dans des scénarios en nuage hybride.

3.3.4 MOBILITÉ DES SERVICES

Au moment de concevoir et de déployer vos services opérationnels, vous pouvez choisir parmi la gamme de services offerts par les FSI en tenant compte à la fois de leurs avantages et inconvénients. Pour demeurer concurrentielle, votre organisation doit être en mesure de réagir rapidement aux demandes du marché et aux exigences des clients. Vous devez adapter votre stratégie de TI de manière à utiliser les services infonuagiques qui répondent le mieux aux besoins de votre organisation, et il pourrait s'agir d'une stratégie hybride à nuages multiples.

Le chiffrement est l'une des pierres angulaires des plateformes infonuagiques du FSI. Si votre organisation veut utiliser plusieurs plateformes infonuagiques, vous devez éviter de dépendre totalement des produits d'un distributeur. Une stratégie de gestion des clés devra être mise en place dans l'ensemble des nombreuses plateformes infonuagiques. Cette stratégie doit tenir compte de la mobilité des services infonuagiques qui sont nécessaires aux environnements en nuage multiples.

Vous pouvez adopter des approches à la gestion des clés comme un service BYOK et un HSM afin de répondre aux exigences liées à la mobilité des services. Votre organisation peut faire appel à un service BYOK pour générer et gérer localement ses clés. La possibilité d'exporter les clés sur les SGC de plusieurs FSI offre la souplesse nécessaire pour migrer les services et les données d'un nuage à l'autre. Dans des environnements assujettis à une réglementation très stricte, recourir à un service BYOK pourrait ne pas constituer une approche acceptable, puisqu'une fois les clés exportées sur les plateformes infonuagiques, il incombe aux FSI d'en assurer le contrôle. Il pourrait être nécessaire de faire appel à des modules HSM dans tels environnements et d'exercer un contrôle distinct sur les données et les clés. En les hébergeant sur le site d'un fournisseur tiers, votre organisation pourra éviter d'avoir à procéder à ce déploiement complexe et tirera avantage de l'agilité qu'offre l'auto-approvisionnement de modules HSM en tant que service. Elle devra toutefois s'assurer qu'elle dispose de la connectivité adéquate pour chaque environnement infonuagique.

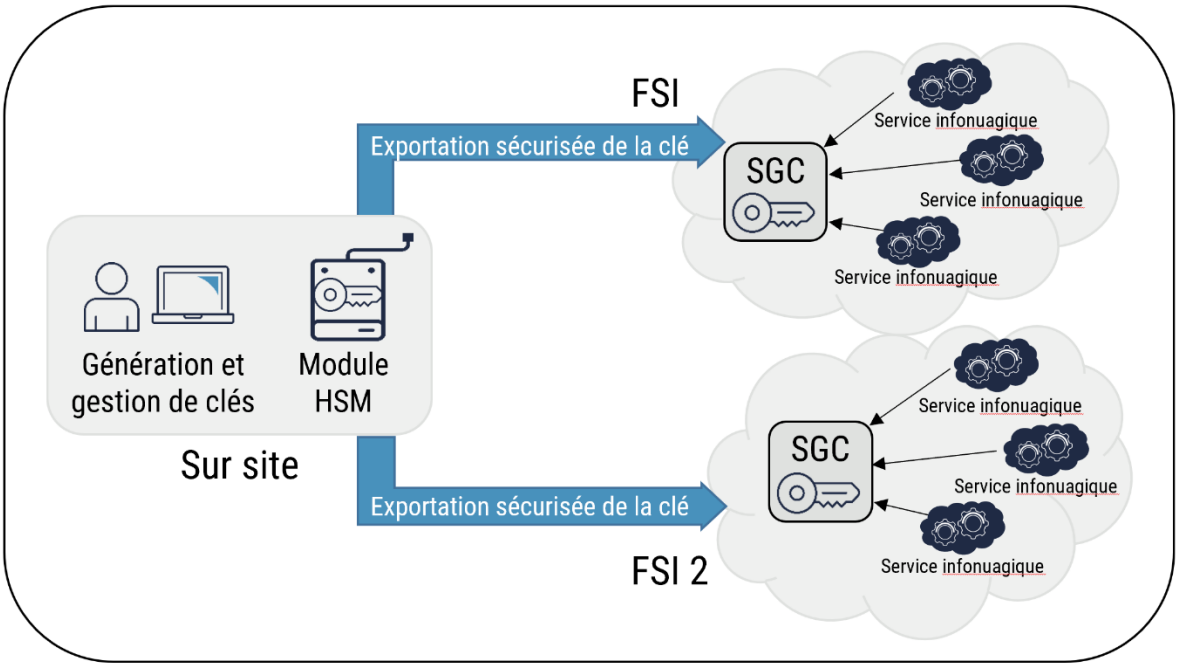

Figure 5 : **Mobilité des services avec BYOK**

3.4 CRYPTO-DÉCHIQUETAGE

Par rémanence des données, on entend la représentation physique résiduelle qui persiste sur un dispositif de stockage malgré les mesures prises pour les éliminer (p. ex., écraser, supprimer ou effacer). Certaines techniques permettent de récupérer les données après leur élimination. La rémanence des données peut mener à la divulgation non intentionnelle d'information sensible si le dispositif de stockage est perdu ou utilisé sans autorisation. Votre organisation devrait protéger la confidentialité des données qui pourraient subsister dans les supports de stockage et en disposer de façon appropriée. Vous devez toutefois vous conformer aux lois (p. ex. les lois sur la protection de la vie privée), aux règlements du gouvernement et de l'industrie, ainsi qu'aux politiques de sécurité de l'organisation.

Selon le document *Special Publication 800-88, Guidelines for Media Sanitization* du NIST [13], le nettoyage des supports est un processus qui consiste à rendre l'accès aux données cibles sur le support impossible selon un niveau d'effort donné. Cette pratique permet de garantir la confidentialité des données qui pourraient subsister dans les supports et de minimiser les risques de divulgation non autorisée. Dans un environnement en nuage multilocataire, les clients de services infonuagiques ne contrôlent pas les supports de stockage physiques. Ils ne peuvent donc pas utiliser les techniques de nettoyage qui exigent un accès physique aux supports. Il faut adopter une autre approche. L'effacement cryptographique (CE pour *Crypto Erase*) est une méthode utilisée pour nettoyer les supports de stockage en nuage avant qu'ils ne soient réintégrés aux ressources partagées du FSI. La version 2 du document ITSP.40.006, *Nettoyage des supports de TI* [14], définit un processus de nettoyage consistant à effacer la clé de chiffrement qui est employée sur un support chiffré pour rendre les données illisibles.

Le recours au chiffrement tout au long du cycle de vie d'un support de stockage accélère et optimise le processus de nettoyage, en plus de simplifier les exigences relatives à la destruction des supports en fin de vie. Les organisations

devraient chiffrer régulièrement tous les supports pendant la durée de leur cycle de vie, de façon à protéger la confidentialité des données, même après que ces supports ont été déclassés et éliminés. Cette pratique permet de garantir la confidentialité des données qui pourraient subsister dans les supports et de minimiser les risques de divulgation non autorisée.

3.5 CHIFFREMENT DU STOCKAGE EN NUAGE

Le stockage en nuage repose sur l'allocation d'un groupe d'unités de stockage logiques et virtuelles aux clients du service infonuagique à partir de ressources partagées physiques. Il incombe également au FSI responsable de l'allocation des ressources de stockage d'assurer le contrôle et la gestion de ces ressources physiques. Les FSI proposent aux clients des options de configuration et de déploiement qui permettront de protéger la sécurité de leurs données dans le cadre des services de stockage en nuage.

Il en revient à votre organisation de sélectionner et de configurer les diverses fonctionnalités de la sécurité du stockage en nuage. Vous devriez comprendre les avantages de chaque approche, notamment les risques que ces approches permettent d'atténuer.

3.5.1 CHIFFREMENT D'UN SERVICE DE STOCKAGE

Le chiffrement du service de stockage permet de chiffrer toutes les données écrites dans le service de stockage. Le FSI contrôle le moteur de chiffrement et accède au matériel de chiffrement. Dans les situations où le FSI offre des capacités BYOK, le client du service infonuagique peut gérer les clés. Par contre, les clés sont toujours contrôlées par le FSI, puisqu'il doit y accéder pour chiffrer et déchiffrer l'information dans le stockage en nuage.

Cette approche offre des capacités de cryptodéchiquetage et protège les données contre tout accès physique non autorisé ou tout accès par d'autres locataires du nuage. Elle procure également une protection additionnelle advenant le vol ou la perte de disques physiques, ou si des utilisateurs non autorisés y accèdent. Toutefois, le chiffrement de services de stockage ne permet pas de protéger les données après leur sauvegarde au moyen des services de sauvegarde en nuage. Votre organisation doit donc veiller à ce que le service qu'il utilise à cette fin assure le chiffrement des données.

3.5.2 CHIFFREMENT AU NIVEAU DE L'INSTANCE

Le chiffrement au niveau de l'instance permet de chiffrer tous les fichiers des systèmes d'exploitation ou qui se trouvent sur les disques virtuels. Votre organisation est responsable de la configuration et de la gestion d'un tel chiffrement. Vous pouvez donc décider quels sont les disques virtuels à chiffrer et utiliser des clés de chiffrement différentes pour chacun des disques. Les administrateurs du stockage gèrent généralement le chiffrement du service de stockage, alors que les administrateurs de systèmes responsables des VM gèrent le chiffrement au niveau de l'instance. Une fois mis en œuvre, le chiffrement au niveau de l'instance a une incidence minime sur les performances. Comme c'est le cas pour le chiffrement des services de stockage, le FSI contrôle toujours les clés de chiffrement, puisqu'il doit accéder aux clés afin de chiffrer et déchiffrer l'information au démarrage des VM.

Par ailleurs, le chiffrement au niveau de l'instance renforce la protection dans les cas où les disques virtuels sont sauvegardés ou lorsque des copies non autorisées sont effectuées aux fins d'analyse hors ligne. Cette approche peut être combinée à des mécanismes de protection préamorçage afin de prévenir toute instanciation non autorisée d'une VM.

Le chiffrement au niveau de l'instance ne permet pas de protéger la sauvegarde de fichiers en particulier ou l'accès aux données advenant la compromission de la VM.

On peut utiliser à la fois le chiffrement au niveau de l'instance et le chiffrement des services de stockage. Comme chaque approche peut être gérée par différents rôles et concerne des menaces diverses, le recours à ces deux types de chiffrement s'inscrira dans la stratégie de défense en profondeur de votre organisation.

3.5.3 DONNÉES EN TRANSIT

L'accès réseau au stockage en nuage n'est pas toujours chiffré par défaut. Vous devriez vous assurer que les services de stockage en nuage sont configurés de manière à indiquer que seuls les protocoles sécurisés (p. ex. HTTPS et SMB 3.0) peuvent être utilisés pour accéder aux services de stockage en nuage et aux API.

3.5.4 GESTION DES CLÉS

On accède aux services de stockage en nuage au moyen de clés d'accès. Les clients de services infonuagiques obtiennent les clés de stockage à partir du portail de gestion du FSI.

Votre organisation devrait établir un processus documenté de gestion et de rotation des clés afin de prévenir la divulgation non autorisée des données et des clés d'accès de stockage. Certains services de stockage en nuage vous permettent d'émettre des clés de stockage, lesquelles sont valides dans la mesure où elles sont utilisées dans le délai prescrit, combinées à des protocoles sécurisés et en provenance de plages d'adresses IP en particulier. Il importe de comprendre les options des clés de stockage en nuage fournies par votre FSI. Utilisez toujours les options de gestion de clés qui conviennent aux exigences de protection de l'information imposées par votre organisation.

3.6 CHIFFREMENT DES BASES DE DONNÉES

Votre organisation peut stocker une grande quantité d'informations sensibles dans les bases de données. Cette information est une cible de grande valeur pour les auteurs de menace. Vous devriez vous assurer de mettre en place des mesures de sécurité pour protéger ces bases de données. En déployant les structures des bases de données sur les plateformes en nuage, vous cédez tout contrôle sur les composantes de l'infrastructure sous-jacente qui soutiennent ces bases de données. Un incident de sécurité lié à votre base de données peut avoir des conséquences désastreuses. Il faut prendre en considération ces facteurs au moment d'élaborer et d'autoriser les modèles de conception à utiliser lors du développement des charges de travail infonuagiques.

La cryptographie joue un rôle essentiel dans la prévention de tout accès non autorisé à l'information contenue dans les bases de données et à la divulgation d'une telle information. Elle prend également en charge l'authentification des systèmes d'extrémité et des utilisateurs concernés par les transactions de la base de données, et assure la confidentialité et l'intégrité des données lorsqu'elles sont en transit et inutilisées.

3.6.1 AUTHENTIFICATION

Dans le cas de déploiements en nuage, le trafic réseau entre le serveur des applications et celui des bases de données passe par une infrastructure réseau sur laquelle votre organisation n'a aucun contrôle. Ne pas authentifier chaque extrémité de la connexion entre un serveur d'applications et un serveur de bases de données pourrait exposer le flux de données aux attaques d'auteurs de menace. Ces derniers pourraient intercepter ou relayer les connexions au réseau, ou tenter d'usurper l'identité d'un système source ou d'un utilisateur légitime. Les approches souvent adoptées pour prévenir les attaques de l'intercepteur de ce type consistent à déployer une authentification basée sur une paire de clés publique et privée afin de déterminer l'identité des systèmes d'extrémité qui prennent part aux transactions de la base de données. L'authentification mutuelle de ces systèmes d'extrémité est mise en œuvre au moyen de certificats d'infrastructure à clé publique (ICP) qui permettent d'authentifier les serveurs de bases de données auprès des applications clientes et des utilisateurs. Elle fait également appel aux certificats des clients, à des chaînes de connexion, à des jetons ou aux justificatifs d'identité des bases de données pour authentifier le système client ou l'utilisateur auprès de la base de données. Dans un environnement infonuagique où les clients n'ont aucun contrôle sur l'infrastructure réseau, les systèmes d'extrémité doivent s'authentifier l'un l'autre pour prévenir les attaques de l'intercepteur.

3.6.2 CHIFFREMENT DES DONNÉES EN TRANSIT

Bien qu'il soit primordial d'authentifier les points terminaux qui prennent part aux transactions des bases de données, il est tout aussi important d'assurer la confidentialité et l'intégrité du flux des bases de données entre les points terminaux.
Le flux des données qui circulent sur l'infrastructure réseau entre les environnements locaux et en nuage, et entre les services infonuagiques, peut être modifié ou intercepté, ce qui pourrait avoir une incidence importante sur votre organisation si les mesures de chiffrement appropriées n'ont pas été prises pour la protéger.

Votre organisation devrait imposer l'utilisation des protocoles, des chiffres et des algorithmes de chiffrement réseau mentionnés dans l'ITSP.40.111 [1] pour tous les flux de données entre les services d'applications et de bases de données. Des mesures de chiffrement prenant en compte l'authentification multifacteur doivent également être prises pour protéger la gestion du trafic entre les serveurs d'administration système et les instances de bases de données.

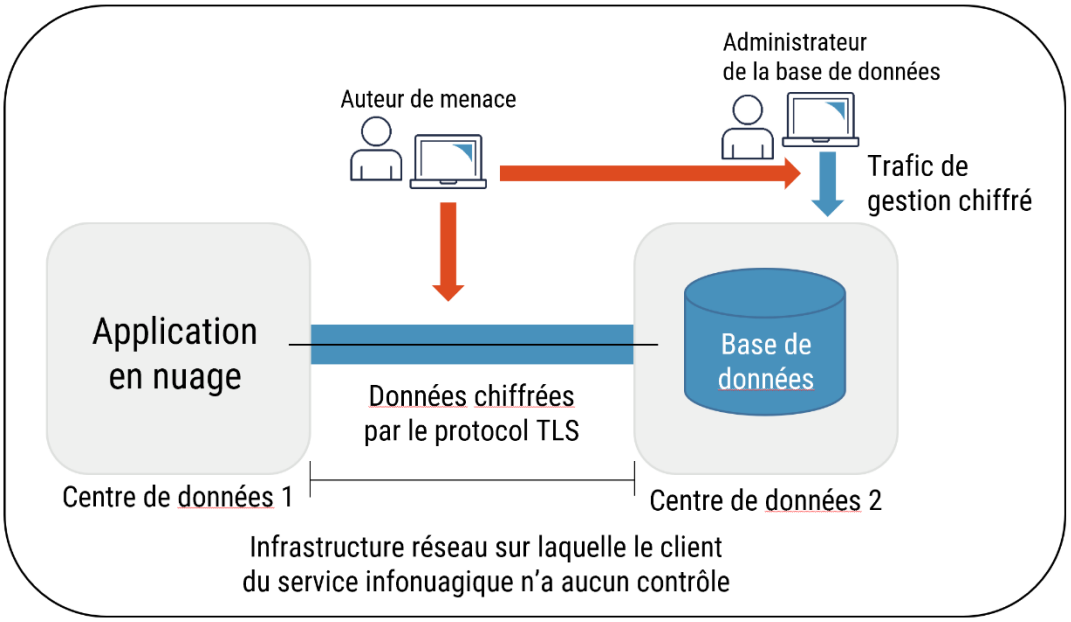

Figure 6 : **Chiffrement des données en transit**

3.6.3 CHIFFREMENT TRANSPARENT DES DONNÉES ET DES BASES DE DONNÉES EXTERNES

Le chiffrement transparent des données (TDE pour *Transparent Data Encryption*) est un processus qui consiste à chiffrer et à déchiffrer les données, les sauvegardes et les fichiers de journalisation au niveau de l'entrée ou de la sortie. Il assure la confidentialité et l'intégrité des données inactives, mais ne protège pas les données utilisées ou en transit. Le TDE permet au serveur de base de données de chiffrer toutes les données écrites sur le disque. Pour ce faire, il n'est pas nécessaire d'apporter des modifications aux applications ou aux schémas de bases de données. Les données sont chiffrées à l'aide d'une seule clé de chiffrement de données (DEK pour *Data Encryption Key*) qui est protégée par d'autres moyens (p. ex. la clé de chiffrement des clés qui est stockée dans la structure des fichiers de bases de données, un HSM ou un SGC).

On peut utiliser le TDE avec le chiffrement de disques ou du stockage. Il protège les données advenant la perte, la copie, le vol ou la modification des fichiers de bases de données, des fichiers de sauvegarde et des supports physiques ou virtuels. Par contre, le chiffrement des disques et du stockage protège uniquement les supports physiques ou virtuels.

Le TDE n'offre aucune protection contre les maliciels, ou encore l'accès ou la modification non autorisés des données par les administrateurs de bases de données. Si des clients de services infonuagiques s'abonnent à la base de données d'une solution PaaS offerte par leur FSI, le personnel du FSI responsable de l'administration de l'instance de bases de données peut potentiellement accéder aux données stockées sur cette base de données. Si l'objectif de votre organisation est de protéger ses données contre les accès non autorisés par des maliciels ou le personnel du FSI, il conviendra d'adopter d'autres approches afin de protéger ses bases de données.

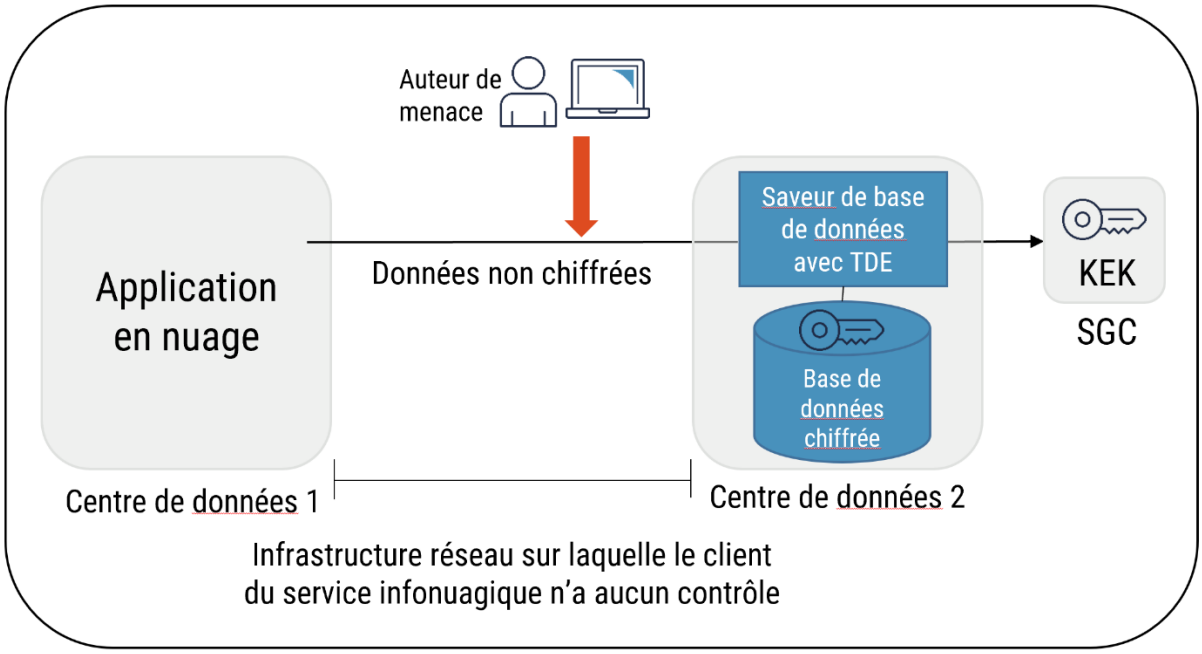

Figure 7 : **Le TDE sans chiffrement des données en transit**

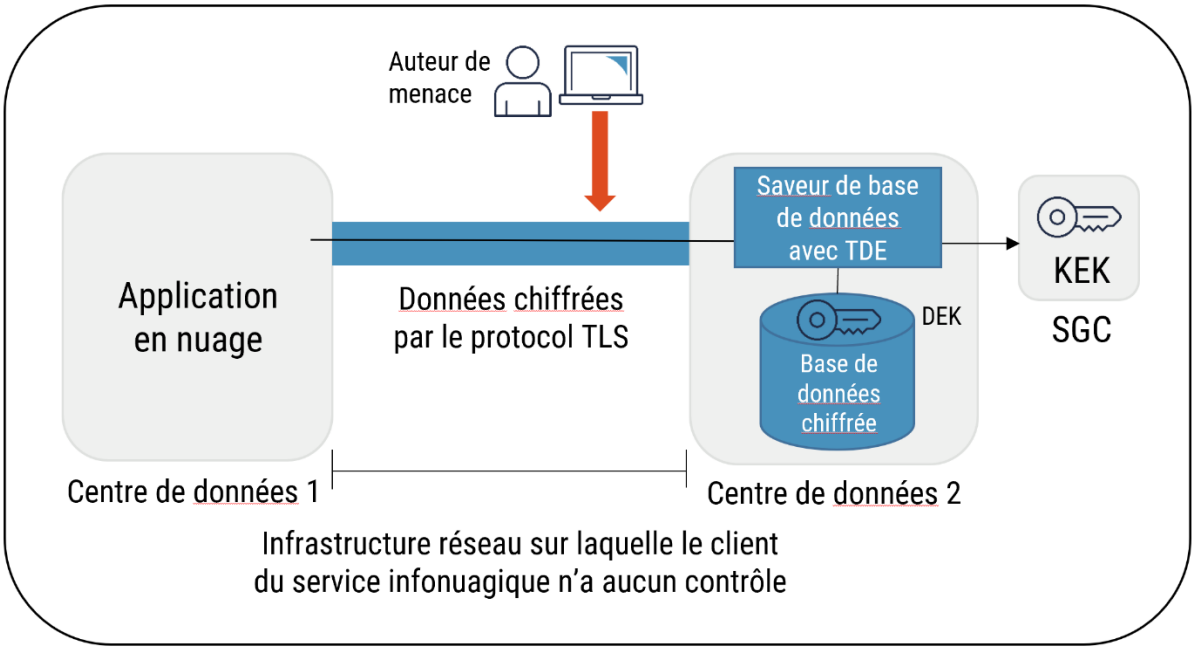

Figure 8 : **Le TDE avec chiffrement des données en transit**

3.6.4 CHIFFREMENT AU NIVEAU DES COLONNES

Le chiffrement au niveau des colonnes facilite la séparation des tâches. Il permet de s'assurer que le personnel (p. ex. les employés du FSI) responsable de la gestion des données stockées dans de grands dépôts (p. ex. des bases de données) est en mesure de les gérer sans avoir à accéder aux données réelles. Grâce au chiffrement au niveau des colonnes, il est également possible de veiller à ce que le personnel devant accéder aux données ne puisse pas accéder aux dépôts de données. Selon ce type de chiffrement, le chiffrement des colonnes est géré par l'application. Cette approche exige que des changements soient apportés aux applications. On peut utiliser les différentes DEK pour chiffrer chaque colonne et les DEK de chaque colonne sont ensuite protégées par d'autres moyens comme un SGC.

Bien qu'il soit nécessaire d'apporter des changements dans les applications, le chiffrement au niveau des colonnes constitue un avantage puisqu'il renforce la sécurité des services infonuagiques. Il s'agit d'un mécanisme de protection dans les cas suivants :

- un membre du personnel du FSI disposant de privilèges élevés tente d'exécuter des requêtes non autorisées sur des bases de données contenant de l'information sensible ou de les modifier;
- un membre du personnel du FSI disposant de privilèges élevés tente d'accéder sans autorisation aux données utilisées de la mémoire ou aux fichiers de l'image mémoire d'un serveur de bases de données, ou de les modifier;
- des maliciels s'exécutant sur les serveurs de bases de données tentent d'accéder aux fichiers, à la mémoire ou aux fichiers de l'image mémoire d'une base de données, ou de les modifier;
- les données en transit entre les serveurs d'applications et de bases de données sont interceptées ou modifiées.

Les clients de services infonuagiques qui s'abonnent aux bases de données d'une solution PaaS peuvent tirer avantage de la sécurité additionnelle offerte par le chiffrement au niveau des colonnes. Un tel renforcement de la sécurité a toutefois une incidence sur les performances et la complexité du processus.

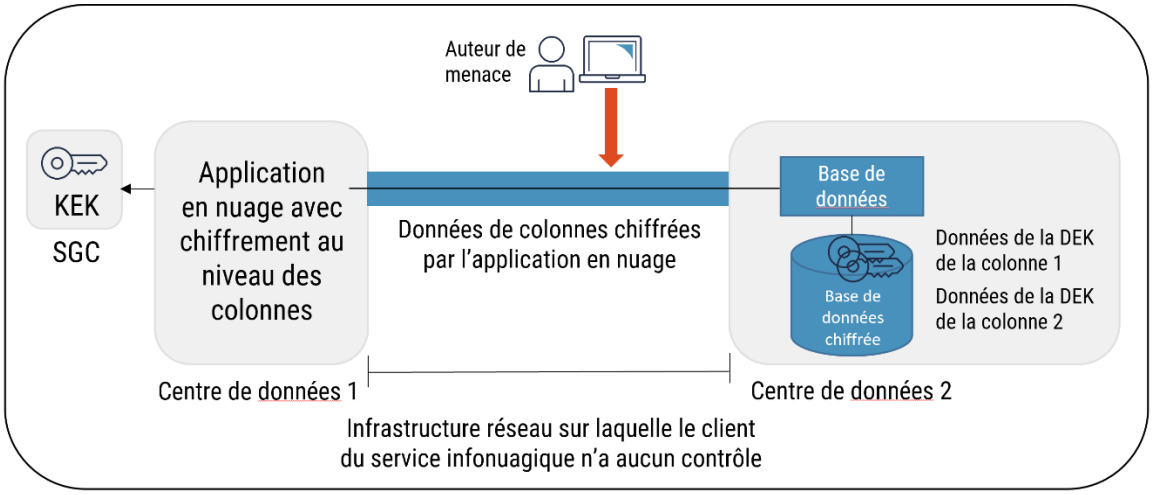

Figure 9 : **Chiffrement de données au niveau des colonnes**

3.6.5 GESTION DES CLÉS

S'ils adoptent les approches au chiffrement des bases de données mentionnées précédemment, les clients de services infonuagiques devraient veiller à ce que la gestion des clés ne soit pas effectuée sur le système qui utilise ces mêmes clés. On recommande fortement aux clients de services infonuagiques d'utiliser un SGC ou des services HSM pour sécuriser le stockage des clés cryptographiques.

3.7 CHIFFREMENT DES POINTS TERMINAUX

Les clients de services infonuagiques dépendent d'une main-d'œuvre de plus en plus mobile pour atteindre leurs objectifs opérationnels. Les clients actuels se servent de plusieurs types de dispositifs (p. ex. téléphones intelligents, tablettes et portables) pour accéder à distance aux applications en nuage. Au même titre que les grands dépôts de données, les points terminaux mobiles constituent l'une des principales cibles des auteurs de menace. La compromission des dispositifs d'extrémité et des justificatifs d'identité offre un point d'entrée idéal vers l'information de votre organisation.

Les clients de services infonuagiques demeurent responsables de la sécurité des points terminaux utilisés pour accéder aux charges de travail et aux données en nuage. Pour garantir une protection adéquate des dispositifs d'extrémité, il importe que les nombreux contrôles mis en place travaillent de concert pour assurer la sécurité des points terminaux, des données et des justificatifs d'identité. Le chiffrement joue un rôle de plus en plus important dans la protection des dispositifs d'extrémité et les clients de services infonuagiques doivent veiller à ce que la configuration des capacités de chiffrement sur les points terminaux mobiles soit gérée efficacement, notamment :

- s'assurer que les algorithmes de chiffrement, les chiffres et les protocoles sont configurés et respectés;
- veiller à ce que les flux de données de gestion des agents d'extrémité et des dispositifs mobiles soient authentifiés et chiffrés;
- protéger les données inutilisées en chiffrant les disques, les fichiers et les dispositifs de stockage amovibles (p. ex., clés USB).

Votre organisation devrait veiller à maintenir la confidentialité et l'intégrité de ses données en faisant appel à des applications configurées de manière à utiliser des protocoles et algorithmes approuvés.

4 RÉSUMÉ

Le présent document peut vous aider à comprendre les éléments du chiffrement des services infonuagiques qu'il convient de prendre en considération pour assurer l'efficacité d'un programme d'assurance de la sécurité infonuagique.

Pour une mise en œuvre efficace du chiffrement des services infonuagiques, votre organisation doit comprendre les différentes solutions offertes par les services de chiffrement, les approches en la matière, les protocoles, les chiffres et les modèles de gestion des clés disponibles. Une sélection, une mise en œuvre, une configuration et une gestion inappropriées des services et protocoles de chiffrement pourraient donner lieu à des lacunes graves et à une protection inefficace des données et services en nuage.

Votre organisation devrait analyser les options de gestion des clés et de chiffrement de bases de données offertes, puis sélectionner les approches qui correspondent le mieux à votre stratégie de déploiement en nuage, à sa tolérance au risque et à ses exigences de conformité.

4.1 AIDE ET RENSEIGNEMENTS

Pour obtenir de plus amples renseignements sur les évaluations et les autorisations de sécurité des services fondés sur l'infonuagique, prière de communiquer avec l'équipe des Services à la clientèle du Centre pour la cybersécurité :

Centre d'appel du Centre pour la cybersécurité
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

5 CONTENU COMPLÉMENTAIRE

5.1 LISTE DES ABRÉVIATIONS

Terme	Définition
API	Interface de programmation d'applications (*Application Program Interface*)
BYOK	Service Bring your own keys
CASB	Courtier de sécurité d'accès au nuage (*Cloud Access Security Broker*)
Centre pour la cybersécurité	Centre canadien pour la cybersécurité
CE	Effacement cryptographique (*Crypto Erase*)
CEG	Passerelles de chiffrement en nuage (*Cloud Encryption Gateways*)
CSA	Cloud Security [sécurité infonuagique] Alliance
CST	Centre de la sécurité des télécommunications
DEK	Clé de chiffrement de données (*Data Encryption Key*)
FSI	Fournisseur de services infonuagiques
HSM	Module de sécurité matériel (*Hardware Security Module*)
HTTPS	Protocole HTTPS (*Hypertext Transfer Protocol Secure*)
IaaS	Infrastructure en tant que service (*Infrastructure as a Service*)
ICP	Infrastructure à clé publique
IdO	Internet des objets
IP	Protocole Internet (*Internet Protocol*)
KMIP	Protocole KMIP (*Key Management Interoperability Protocol*)
NIST	National Institute of Standards and Technology
PaaS	Plateforme en tant que service (*Platform as a Service*)
PC	Partie de confiance
PCI DSS	Normes de sécurité sur les données de l'industrie des cartes de paiement (*Payment Card Industry Data Security Standard*)
SaaS	Logiciel en tant que service (*Software as a Service*)
SCT	Secrétariat du Conseil du Trésor du Canada
SGC	Système de gestion des clés
SMB	Bloc de messages de serveur (*Server Message Block*)
TDE	Chiffrement transparent des données (*Transparent Data Encryption*)
TI	Technologies de l'information
VM	Machine virtuelle (*Virtual Machine*)

5.2 GLOSSAIRE

Terme	Définition
Assertion	Instruction d'un vérificateur transmise à la partie de confiance. Cette instruction contient l'information d'identité concernant un abonné. Les assertions peuvent également contenir des attributs vérifiés.
Authenticité	Mesure de sécurité destinée à protéger un système contre les transmissions ou les imitations frauduleuses en établissant la validité d'une transmission, d'un message ou de l'expéditeur.
Authentification	Mesure visant à protéger un système contre les transmissions frauduleuses et la simulation, et qui consiste à établir la validité d'une transmission, d'un message ou de l'identité de l'expéditeur.
Chiffrement	Transformation cryptographique des données en une forme qui masque la signification d'origine des données pour qu'on ne puisse pas les connaître ou les utiliser. Si la transformation est réversible, le processus inverse, qu'on appelle « déchiffrement », permettra de restaurer les données chiffrées à leur état initial.
Confidentialité	Fait d'être divulgué uniquement aux mandants autorisés.
Cryptographie	Discipline qui incarne les principes, les techniques et les méthodes de la transformation de données qui visent à dissimuler le contenu sémantique, ainsi qu'à prévenir les modifications non détectées et une utilisation non autorisée.
Déchiffrement	Conversion en clair de l'information (voix ou données) chiffrée par l'opération inverse du chiffrement.
Disponibilité	Condition d'être accessible et utilisable de manière fiable et en temps opportun.
Gestion des clés	Procédures et mécanismes de génération, de distribution, de remplacement, de stockage, d'archivage et de destruction des clés qui commandent les processus de chiffrement ou d'authentification.
Intégrité	Exactitude et intégralité de l'information et des biens, et authenticité des transactions.
Internet des objets	Concept qui consiste à étendre la connectivité Internet au-delà des plateformes informatiques traditionnelles, comme les ordinateurs personnels et les appareils mobiles, pour tenir compte d'une gamme d'objets du quotidien et de dispositifs anciennement « bêtes » ou non connectés à Internet.
Protocole KMIP	Permet la communication entre les systèmes de gestion des clés et les applications faisant appel au chiffrement, comme les courriels, les bases de données et les dispositifs de stockage. Selon la définition fournie par OASIS, le protocole KMIP est un protocole de communication servant à établir la communication entre les clients et les serveurs pour exécuter certaines opérations de gestion sur des objets stockés et gérés par un système de gestion des clés.

5.3 RÉFÉRENCES

Numéro	Référence
[1]	Centre pour la cybersécurité. ITSP.40.111, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B*, août 2016.
[2]	Centre pour la cybersécurité. ITSP.40.062, *Conseils sur la configuration sécurisée des protocoles réseau*, août 2016.
[3]	SCT. *Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS)*, 1er novembre 2017.
[4]	Centre pour la cybersécurité. ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2014.
[5]	CSA. *Security Guidance for Critical Areas of Focus in Cloud Computing*, version 4.0, 2017.
[6]	NIST. *Computer Security Resource Centre Glossary*, non daté.
[7]	Centre pour la cybersécurité. ITSP.30.031, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information*, version 3, avril 2018.
[8]	Centre pour la cybersécurité. ITSP.50.103, *Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique*, 2019.
[9]	Centre pour la cybersécurité. ITSP.50.105, *Guide sur l'évaluation et l'autorisation de la sécurité infonuagique*, 2019.
[10]	NIST. *Special Publication 800-57 Recommendation for Key Management, Part 1: General (Revision 4)*, 28 janvier 2016.
[11]	Conseil des normes de sécurité PCI. *PCI DSS Cloud Computing Guidelines*, avril 2018.
[12]	SCT. *Gouvernement du Canada, Livre blanc : Souveraineté des données et nuage public*, non daté.
[13]	NIST. *Special Publication 800-88 Guidelines for Media Sanitization (Revision 1)*, 18 décembre 2014.
[14]	Centre pour la cybersécurité. ITSP.40.006, *Nettoyage des supports de TI*, version 2, juillet 2017.