IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

Stratégie de chiffrement des identifiants des clients

Version ~~1.7.0~~1.8.1
~~20 mai~~11 août 2020

Historique du document

Version	Description des modifications	Date
1.0	• Création du document. Première version provisoire terminée.	5 juin 2019
1.1	• Modifications mineures	15 juillet 2019
1.2	• Modifications et clarifications à la suite des commentaires du comité de mise en œuvre	2 septembre 2019
1.3	• Expansion du processus de gestion des clés	5 novembre 2019
1.4	• Révision de la section 2.2 Chiffrement des valeurs FIX par l'ajout de l'encodage Base64 • Mise à jour de la figure 2 Structure de la valeur chiffrée • Ajout de la figure 3 Calendrier de rotation des clés	2 décembre 2019
1.5	• Précision : Le code du courtier peut être composé de 3 caractères plutôt que d'un numéro à 3 chiffres • Précision : La randomisation du bloc compteur n'est pas obligatoire	20 janvier 2020
1.6	• Mise à jour de la section Gestion des clés	11 mars 2020

1.7	• Mise à jour de la section 2.2 Chiffrement des valeurs FIX : Le nombre aléatoire et le bloc compteur ont été remplacés par le vecteur d'initialisation
	• Mise à jour de la section 2.3 Gestion des clés
	  ○ Avant d'être envoyée, la clé est chiffrée en texte de 24 caractères au moyen de l'encodage Base64
	  ○ La clé est envoyée par courriel sécurisé
	  ○ Le courtier accuse réception de la clé à l'aide du lien URL fourni dans le courriel
		20 mai 2020

1.8	• Mise à jour de la figure 2 – Structure de la valeur chiffrée – afin que les exemples de données dans la figure soient des données réelles aux fins de référence aux tests de mise en œuvre	11 août 2020

Table des matières

1. Au sujet du présent document

1.1 Introduction

L'OCRCVM a modifié les Règles universelles d'intégrité du marché (RUIM) afin que les identifiants des clients et certaines désignations soient dorénavant indiqués pour l'ensemble des ordres sur titres cotés envoyés à un marché et l'ensemble des opérations qui en résultent. Les identifiants des clients seront chiffrés par le courtier membre duquel proviennent les ordres afin que seule l'autorité de réglementation voie les identifiants (et non les marchés). Le présent document énonce la méthode de chiffrement et l'infrastructure connexe requise pour réussir sa mise en œuvre (présentation du texte chiffré sur le signal FIX, gestion des clés, etc.).

1.2 Public visé

Le présent document a été initialement rédigé pour le comité de mise en œuvre des identifiants des clients de l'OCRCVM, mais pourrait être utilisé plus tard par le personnel de la sécurité de l'information, des analyses opérationnelles, du perfectionnement et de l'assurance de la qualité qui joue un rôle dans la mise en œuvre du chiffrement des identifiants des clients.

2. Méthode de chiffrement

2.1 Norme de chiffrement avancé (AES)

La norme de chiffrement avancé (AES) est une spécification de chiffrement de données électroniques qui a été établie par le National Institute of Standards and Technology des États-Unis (NIST). Cette norme est maintenant utilisée à l'échelle internationale, et elle a trait au seul chiffrement publiquement accessible approuvé par la National Security Agency (NSA). Elle a également été adoptée par les États-Unis à titre de norme du gouvernement fédéral en 2002.

La norme AES est un algorithme symétrique de chiffrement par bloc (c.-à-d. que la même clé est utilisée pour le chiffrement et le déchiffrement). La taille des clés peut faire 128, 192 ou 256 bits. L'utilisation de clés de 128 bits réduirait au minimum l'impact sur le rendement du système tout en maintenant un degré de sécurité de l'information suffisant.

2.1.1 Mode d'opération – norme AES-mode CTR

Un mode d'opération est un algorithme utilisé conjointement avec un chiffrement par bloc pour améliorer la sécurité de l'information. Il existe une grande variété de modes qui comportent un éventail de garanties de sécurité et d'efficacité; le mode compteur (mode CTR) offre de nombreux avantages en matière d'efficacité par rapport à d'autres modes, sans toutefois affaiblir la sécurité (p. ex. il est hautement parallélisable et passe de manière sécuritaire d'un chiffrement par bloc à un chiffrement par flot – le remplissage n'est alors plus nécessaire).

Le texte en clair est d'abord divisé en blocs que l'algorithme de base combine à un nombre aléatoire (ou un « vecteur d'initialisation ») – une valeur arbitraire impossible à prévoir générée de manière aléatoire ou pseudo-aléatoire – et à un compteur qui progresse à chaque bloc. Cette combinaison est ensuite chiffrée au moyen d'une clé, et un XOR est appliqué au résultat avec le texte en clair pour générer le texte chiffré. La figure 1 décrit le processus de manière simplifiée.

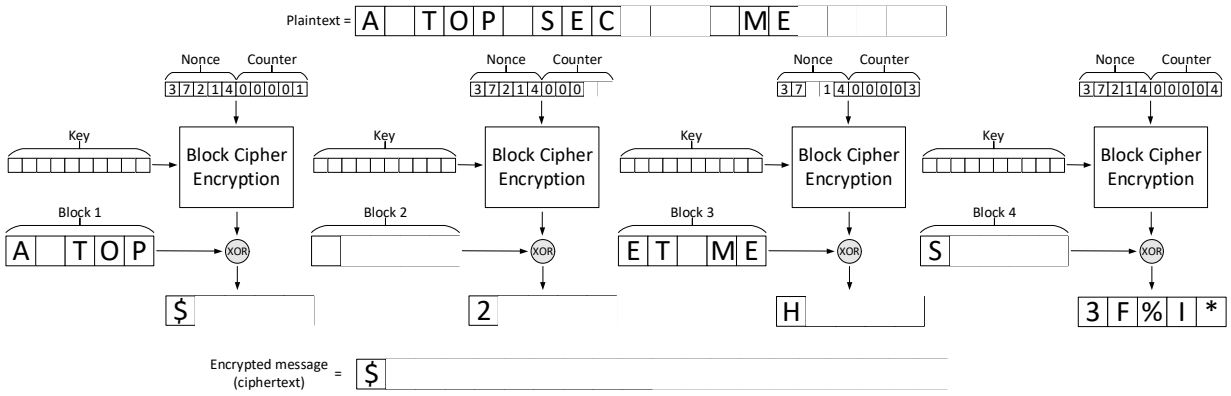

Figure 1 : Chiffrement norme AES-mode CTR

2.2 Chiffrement des valeurs FIX

Les champs FIX pertinents devraient contenir une chaîne composée de trois éléments concaténés :

- un code de 3 octets unique identifiant le courtier membre à l'origine du chiffrement;
- un vecteur d'initialisation de 16 octets;
- la valeur chiffrée de 20 octets du LEI.

Les données binaires concaténées sont ensuite encodées au moyen de Base64 pour former une chaîne de 52 caractères attribués au champ FIX pertinent, comme le montre la figure 2 ci-dessous :

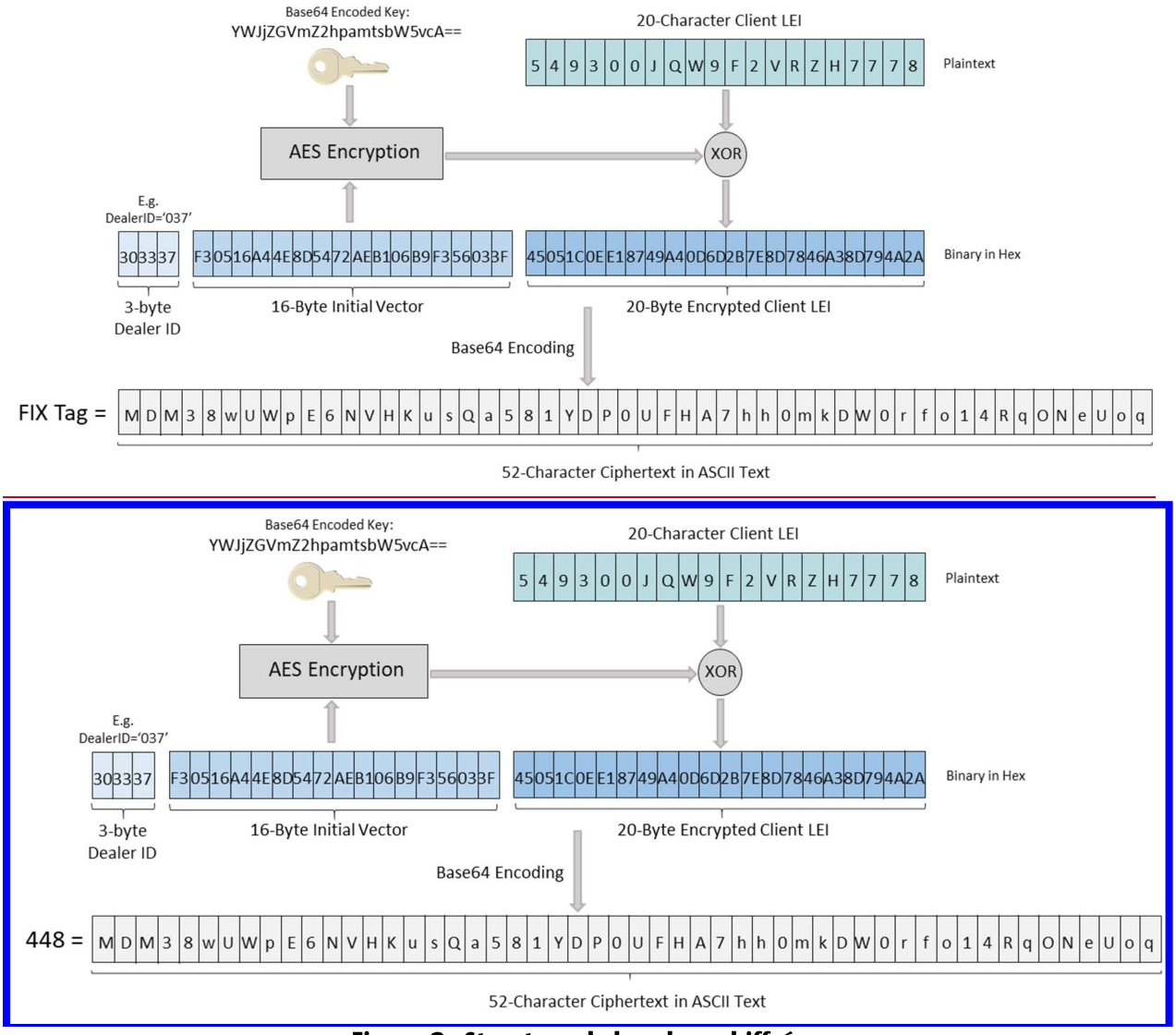

Figure 2 : Structure de la valeur chiffrée

- La clé de chiffrement est de 16 octets et est chiffrée en texte de 24 caractères au moyen de l'encodage Base64;
- Le vecteur d'initialisation est un bloc de 128 bits (16 octets) stocké selon une architecture petit-boutiste;
- Nous recommandons de générer le vecteur d'initialisation de manière aléatoire, de façon à ce qu'un vecteur d'initialisation unique et impossible à prévoir soit attribué à chaque ordre. Ainsi,

des textes chiffrés distincts seront générés pour le LEI d'un même client dans des ordres différents, puisque chaque combinaison d'une clé et d'un vecteur d'initialisation sera utilisée une seule fois;

- Il n'est cependant pas obligatoire de générer le vecteur d'initialisation de façon aléatoire pour chaque ordre. On peut utiliser un seul vecteur d'initialisation pour chiffrer le LEI d'un client. Dans ce cas, le client doit comprendre que le LEI chiffré qui sera attribué à tous ses ordres et vu par les marchés sera formé de la même chaîne de caractères.
- Le code du courtier à l'origine du chiffrement permet à l'OCRCVM de déterminer la clé de déchiffrement appropriée pour un LEI donné. Ce code sera attribué au moment de la diffusion des clés de chiffrement initiales;
- Le code du courtier concaténé, le vecteur d'initialisation et le LEI chiffré du client constituent des données binaires arbitraires de 39 octets qui doivent ensuite être transformées en texte ASCII lisible de 52 caractères au moyen de l'encodage Base64;
- Lorsqu'un participant exécutant reçoit un ordre d'un courtier membre non exécutant qui souhaite exécuter un ordre pour son client et que le LEI du client n'est pas chiffré, il doit se servir de sa propre clé de chiffrement pour chiffrer le LEI. Un participant exécutant peut déterminer si un LEI est chiffré ou non (et, par conséquent, s'il doit utiliser sa propre clé de chiffrement ou non) en examinant la longueur du champ LEI dans le message transmis par le courtier membre non exécutant. Ainsi, si le champ contient plus de 20 caractères (20 caractères étant la longueur d'un LEI non chiffré), le participant peut présumer que le LEI a déjà été chiffré par le courtier membre non exécutant.

2.3 Gestion de la rotation des clés

Une clé de chiffrement différente sera remise à chaque courtier membre duquel proviennent les ordres. La clé, composée de données binaires de 128 bits, sera chiffrée en texte ASCII de 24 caractères au moyen de l'encodage Base64 et envoyée au courtier membre par courriel chiffré. Les clés seront actualisées tous les 12 mois. L'OCRCVM générera et distribuera les clés une fois par année (plutôt que de distribuer en même temps des clés valides pour plusieurs années). Nous croyons que cette approche réduira au minimum l'incertitude potentielle à propos du moment de l'actualisation des clés, de leur utilisation, etc.

Le calendrier de rotation des clés fonctionnera comme l'illustre la figure 3 :

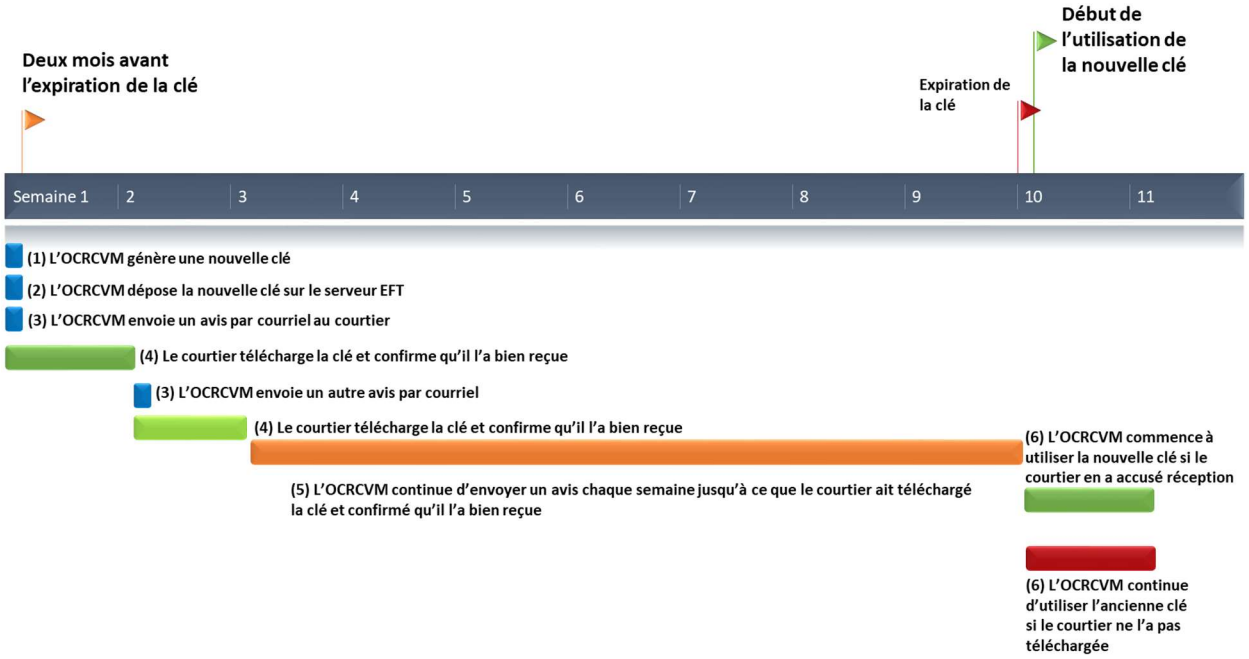

Figure 3 : Calendrier de rotation des clés

1. Deux mois avant l'expiration de la clé, l'OCRCVM en générera une nouvelle pour chaque courtier membre actif.
2. La nouvelle clé est chiffrée en texte ASCII de 24 caractères au moyen de l'encodage Base64 et conservée dans un fichier texte nommé selon le modèle xxx_aaaammjj_aaaammjj.key, où :
    - xxx est le code de courtier unique à 3 caractères;
    - La première valeur aaaammjj est la date d'activation de la nouvelle clé;
    - La deuxième valeur aaaammjj est la date d'expiration de la nouvelle clé.
3. L'OCRCVM utilisera le protocole sécurisé TLS pour envoyer au courtier membre un courriel (avec le fichier texte en pièce jointe) l'avisant que sa nouvelle clé est prête à être téléchargée.
4. Chaque courtier membre recevra un courriel contenant un lien URL temporaire (valide pour une semaine) unique pour chaque nouvelle clé. L'administrateur de la clé chez le courtier membre doit cliquer sur le lien pour accuser réception de la nouvelle clé de chiffrement.
5. Une fois que le courtier membre accusera réception de la nouvelle clé, l'OCRCVM s'attend à ce qu'il effectue toutes ses opérations :
    a) en continuant d'utiliser la clé existante jusqu'à ce qu'elle expire;
    b) en commençant à utiliser la nouvelle clé dès qu'elle est activée.
6. Si le courtier membre omet de cliquer sur le lien URL contenu dans le courriel dans la semaine suivant l'avis, un nouveau courriel sécurisé, avec la clé chiffrée en pièce jointe, lui sera envoyé. Par la suite, il recevra un rappel chaque semaine s'il ne clique pas sur le lien URL contenu dans le courriel.
7. L'OCRCVM utilisera les nouvelles clés pour déchiffrer le LEI du client à compter de leur date d'activation.